Indiana Law Review

Volume 43 **2010** **Number 2**

ARTICLES

PHYSICIANS AND PATIENTS WHO "FRIEND" OR "TWEET": CONSTRUCTING A LEGAL FRAMEWORK FOR SOCIAL NETWORKING IN A HIGHLY REGULATED DOMAIN

NICOLAS P. TERRY*

Introduction 286
I. Social Networks 288
A. *Properties of Social Networks* 289
B. *Use, Perceptions, and Expectations* 292
C. *Social Network Privacy and Security Settings* 294
II. The Legal (and Not So Legal) Framework 297
A. *Options; Property, Liability, Inalienability, and Soft Law* 299
B. *The Law of Boundaries; Privacy Torts and Breach of Confidence* 301
1. Intrusion upon Seclusion 302
2. Public Disclosure of Private Facts 303
3. Breach of Confidence 304
C. *Privacy Expectations and Social Networks* 305
D. *Privacy and Confidentiality in Healthcare* 307
1. Intrusion Actions 308
2. Publicity Actions 309
3. Confidentiality Actions 313
E. *Ethical Restraints* 314
F. *HIPAA and Related Regulatory Models* 316
III. Setting Boundaries for Physicians and Patients 318
A. *Physicians' Social Information Online* 319
B. *Patients' Health-Related Information Online* 322
1. Employers and Insurers 323
2. Physician Use of Posted Social Information 325
3. Third Parties Posting Patient Information 326
C. *Physicians and Patients as "Friends"* 329
1. Creating a Physician-Patient Relationship 330
2. Risk-Managing a Blurred Relationship 333
3. Appropriateness of "Friend" Relationships 334

* Chester A. Myers Professor of Law, Senior Associate Dean, Saint Louis University, email: terry@slu.edu. I thank Leslie Francis for her helpful suggestions on an earlier draft and Michael Kella, J.D. Candidate, 2011, Saint Louis University, and Professor Margaret McDermott of our law library faculty for their research assistance.

D. Physicians "Tweeting" or Posting About Their Work 335
1. Blogging and Posting 336
2. Twitter Feeds and Status Updates 338
Conclusion 340

"If Relationship George walks through this door, he will kill Independent George! A George divided against itself cannot stand!"[1]

INTRODUCTION

Computer-mediated social network sites are omnipresent and among the most popular of all web destinations. There seem to be few limits on who is posting or the subject matter of posts, and there is scant guidance on the appropriate limits for online social interactions. Originally, such sites were the exclusive playground of teenagers and college students (who continue to be the majority of users).[2] Not surprisingly given this original demographic, media and legal scrutiny concentrated on the potential of such sites to enable child predators,[3] facilitate other abuses of children and young adults such as bullying,[4] and encourage graffiti behavior in adolescent users.[5]

Although teenagers and young adults remain the dominant groups using social network sites, adult usage quadrupled between 2005 and 2008[6] as adults migrated to Facebook and MySpace initially, perhaps, to connect with their children and grandchildren.[7] By December 2008, 35% of online adults had used a social network site.[8] Of course, all users do not equally enjoy all social network activities. For example, updating one's personal status using Twitter or Facebook's "What's on your mind?" feature continues to be an activity

---

1. *Seinfeld: The Pool Guy* (NBC television broadcast Nov. 16, 1995).

2. Amanda Lenhart, ADULTS AND SOCIAL NETWORK WEBSITES, PEW INTERNET & AMERICAN LIFE PROJECT (2009), http://www.pewinternet.org/~/media//Files/Reports/2009/PIP_Adult_Social_networking_data_memo_FINAL.pdf.pdf.

3. *See, e.g.*, Doe v. MySpace Inc., 528 F.3d 413 (5th Cir.), *cert. denied*, 129 S. Ct. 600 (2008).

4. *See, e.g.*, United States v. Drew, No. CR 08-0582-GW, 2009 WL 2872855 (C.D. Cal. Aug. 28, 2009); Lauren Collins, *Friend Game: Behind the Online Hoax That Led to a Girl's Suicide*, NEW YORKER, Jan. 21, 2008, *available at* http://www.newyorker.com/reporting/2008/01/21/080121fa_fact_collins; Alexandra Zavis, *MySpace Conviction in Doubt*, L.A. TIMES, July 3, 2009, at A3, *available at* 2009 WLNR 12700576.

5. *See infra* notes 136-49 and accompanying text (cases involving, for example, schoolchildren posting abusive materials about their schools or teachers).

6. Lenhart, *supra* note 2, at 1.

7. John D. Sutter, *All in the Facebook Family: Older Generations Join Social Networks*, CNN.COM, Apr. 13, 2009, http://www.cnn.com/2009/TECH/04/13/social.network.older/.

8. Lenhart, *supra* note 2, at 1; *see also* Sutter, *supra* note 7.

dominated by young adults.[9]

Online social networks are increasingly attracting the attention of large and small businesses and professionals as vehicles for advertising, marketing, and providing customer support.[10] For example, 54% of attorneys belong to an online social network,[11] although membership remains skewed towards younger professional users.[12] As the demographics of and motivations behind participation in social networks evolve, the foundational teenager versus teenager relationships and inevitable disputes will be replaced by more complex relationships and risks that are considerably more nuanced.

This Article focuses on one highly complex relationship, that of physician and patient. That relationship, together with the related imperative of protecting patient information, constitutes a crucial component of the legal domain applicable to our most highly regulated industry. Recent inquiries into the trust and confidence properties of the physician-patient relationship and the protection of patient data concentrated on the technical (diagnostic, pharmacy, etc.) data associated with the care relationship. Thus, questions have been asked about the adequacy of protection for networked or interoperable electronic records.[13] Such inquires have escalated as patients have been encouraged to leverage technology to store their own "personal" health records.[14] This Article is less interested in technical medical data and more with *social* data that implicates health and

---

9. AMANDA LENHART & SUSANNAH FOX, TWITTER AND STATUS UPDATING, PEW INTERNET & AMERICAN LIFE PROJECT 1 (2009), *available at* http://www.pewinternet.org/~/media//Files/Reports/2009/PIP%20Twitter% 20Memo%20FINAL.pdf.

10. *See, e.g.*, Posting of Douglas A. McIntyre to 24/7 WallSt.com, http://247wallst.com/2009/05/26/the-ten-ways-twitter-will-permanently-change-american-business (May 26, 2009, 20:11 EST); *see also* Nicola Clark, *Airlines Follow Passengers Onto Social Media Sites*, N.Y. TIMES, July 29, 2009, http://www.nytimes.com/2009/07/30/business/global/30tweetair. html; Amy Miller, *FMC Turns to Social Networking to Find Law Firms*, LAW.COM, May 18, 2009, http://www.law.com/jsp/ihc/PubArticleIHC.jsp?id=1202430756051 (discussing use by client to increase its pool of potential outside counsel through post on *Legal OnRamp*, a social network for lawyers); Richard Raysman & Peter Brown, *Behavioral Ads: Social Networks' Latest Legal Pitfall?*, LAW.COM, Mar. 25, 2008, http://www.law.com/jsp/lawtechnologynews/pubArticleLT.jsp? id=900005506762; Jason Snell, *Nine Twitter Tips for Business: How to Strike the Right Balance When Using This Popular Messaging Service*, MACWORLD, May 4, 2009, http://www.macworld.com/article/140254/2009/05/twitterdos.html.

11. *Survey Reveals Growth in Online Professional Networking Among Legal Professionals, Appetite for Lawyer-Specific Networking Solutions*, July 10, 2008, http://www.businesswire.com/news/home/20080710005598/en.

12. *Id.* (reporting membership of 25-35 (67%), 36-45 (49%), and 46-55+ year olds (36%)).

13. *See* Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 691-96; *see also* Leslie P. Francis, *The Physician-Patient Relationship and a National Health Information Network*, J.L. MED. & ETHICS (forthcoming).

14. *See generally* Nicolas P. Terry, *Personal Health Records: Directing More Costs and Risks to Consumers?*, 1 DREXEL L. REV. 216 (2009).

health-related decision-making. Here, the inquiry is how our legal, ethical, and regulatory models will react as the social network phenomenon overlaps with traditional healthcare relationships and businesses.

The analysis draws on the limited extant law dealing specifically with social network interactions and the law and ethics literature dealing with existing computer-mediated interactions between physicians and patients. The legal analysis principally is concerned with privacy and confidentiality constructs, described below as the "Law of Boundaries." The Article explores how participation in online social networks may blur boundaries between personal and professional relationships or commentary, while making available "private" information in what only appears to be a secluded area. The Article also examines the potential for amelioration of risks with the currently under-utilized privacy and security settings provided by the online social networks.

The Law of Boundaries is applied to some specific scenarios where category breakdown may be detected: (1) physician social information online, (2) patient health-related information online, (3) physicians and patients as "friends," and (4) physicians "tweeting" or posting about their work. These online scenarios challenge the perceptions, expectations, and sense of trust that are the properties of the offline physician-patient relationship. The application of legal, ethical, and regulatory models to these "worlds collide" phenomena casts doubts on the appropriateness of some professional activities and the online social activities of some physicians. Additionally, the Article identifies the considerable risks run by online patients who post about or otherwise signal their health status. Among several conclusions applicable to these social network scenarios it is suggested that the Law of Boundaries must evolve to protect non-public data or secluded areas established by users of social network sites.

I. SOCIAL NETWORKS

The most popular social network sites include Facebook, MySpace, Twitter, and LinkedIn.[15] Facebook has in excess of 250 million registered users[16] and its subscribers spend more than three billion minutes per day on the web site.[17] Of these services Facebook[18] and Twitter[19] currently show the largest growth.

---

15. Posting of Andy Kazeniac to Compete.com, http://blog.compete.com/2009/02/09/facebook-MySpace-twitter-social-network/ (Feb. 9, 2009).

16. Erick Schonfeld, *Facebook Is Now the Fourth Largest Site in the World*, TECHCRUNCH, Aug. 4, 2009, http://www.techcrunch.com/2009/08/04/facebook-is-now-the-fourth-largest-site-in-the-world (reporting 340 million unique visitors).

17. Owen Thomas, *Facebook at 5: What the Future Holds*, Feb. 4 2009, http://valleywag.gawker.com/5145975/facebook-at-5-what-the-future-holds.

18. *See* Schonfeld, *supra* note 16.

19. Kelly Gregor, *Twitter Takes Top Growth Spot*, NAT'L BUS. REV. 24/7, Jan. 27, 2010, http://www.nbr.co.nz/article/twitter-takes-top-growth-spot-117639. *Compare* Top 10 Social-Networking Websites & Forums—February 2009, http://www.marketingcharts.com/interactive/top-10-social-networking-websites-forums-february-2009-8286/ (showing that Twitter was not a top

Eleven percent of online American adults use Twitter or features on social network service sites to share information or read "updates" from others.[20] The use of social network sites is now so pervasive that we may well be on our way to what Anita Allen described as "the technological conceit of twenty-first century 'lifelogging.'"[21]

Our contemporary concept of social networking is a subset of computer-mediated (or computer network-mediated) communication. This latter, broader term includes email, blogs, web sites, and instant messaging.[22] These extant models of computer network-mediated communication will inform the discussion that follows. However, they lack the distinctive features of social network services.

A. Properties of Social Networks

According to one court, "[o]nline social networking is the practice of using a Web site or other interactive computer service to expand one's business or social network."[23] Boyd and Ellison provide a granular definition: "[W]eb-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."[24]

There are two broad categories of computer-mediated social networks. First, there are those, like LinkedIn,[25] that emphasize professional or business

---

ten social networking site in Feb. 2009), *and* Marketing Charts, Top 10 Social-Networking Websites & Forums—March 2009, http://www.marketingcharts.com/interactI've/top-10-social-networking-websites-forums-february-2009-2-8749/ (showing that by March 2009 Twitter was the eighth most popular social networking site), *with* Marketing Charts, Top 10 Social-Networking Websites & Forums—October 2009, http://www.marketingcharts.com/interactive/top-10-social-networking-websites-forums-october-2009-11099/ (showing that Twitter was the sixth most popular social networking site in October 2009).

20. LENHART & FOX, *supra* note 9, at 1.

21. Anita L. Allen, *Dredging up the Past: Lifelogging, Memory, and Surveillance*, 75 U. CHI L. REV. 47, 48 (2008).

22. A more expansive list of social network services or sites could be drawn up. For example, for some the fact that viewers rate content on YouTube, share opinions about products on Amazon.com, or rate each other on Ebay.com might qualify these sites as social networks.

23. Doe v. MySpace Inc., 528 F.3d 413, 415 (5th Cir.), *cert. denied*, 129 S. Ct. 600 (2008); *see also* Liveuniverse, Inc. v. MySpace, Inc., No. CV 06-6994 AHM CRZx, 2007 WL 6865852 (RZx), at *1 (C.D. Cal. June 4, 2007) ("Social networking websites allow visitors to create personal profiles containing text, graphics, and videos, as well as to view profiles of their friends and other users with similar interests."), *aff'd*, 304 F. App'x 554 (9th Cir. 2008).

24. danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMMC'N, at art. 11 (2007), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

25. *See About Us*, http://press.linkedin.com/about (last visited Feb. 8, 2010) ("LinkedIn is

networking. Second, there are those, such as Bebo[26] (a site popular in Europe[27]), MySpace,[28] and Facebook,[29] which leverage the social or friendship properties of pre-existing, predominately offline networks of intimates, friends, and acquaintances.

Boyd and Ellison explain this distinction between networking and networks as follows:

> What makes social network sites unique is not that they allow individuals to meet strangers, but rather that they enable users to articulate and make visible their social networks. . . . [P]articipants are not necessarily "networking" or looking to meet new people; instead, they are primarily communicating with people who are already a part of their extended social network.[30]

Thus, a typical LinkedIn subscriber seeks to leverage the contacts of contacts to increase the range of their professional networking. But a Facebook user primarily seeks to communicate with an existing network of friends. These users only incidentally (or at least initially), leverage the virtual networks of his or her friends to identify and then "friend" participating friends from their existing real world network.[31] Empirical data seems to bear out this distinction. Adults use professional sites sparingly (e.g., 6% of adults use LinkedIn), but they use them almost exclusively for professional purposes. Social network sites such as Facebook and MySpace see more mixed use, but adults tend to use them far more

---

an interconnected network of experienced professionals from around the world, representing 150 industries and 200 countries. You can find, be introduced to, and collaborate with qualified professionals that you need to work with to accomplish your goals.").

26. *See* bebo.com, About Bebo, http://www.bebo.com/c/about (last visited Feb. 8, 2010) ("Bebo is a popular social networking site which connects you to everyone and everything you care about. It is your life online—a social experience that helps you discover what's going on with your world and helps the world discover what's going on with you.").

27. *See* Geoff Duncan, *Bebo Launches Five European Localizations*, DIGITAL TRENDS, Mar. 16, 2009, http://digitaltrends.com/international/bebo-launches-five-european-localizations.

28. *See* MySpace Quick Tour, http://www.MySpace.com/index.cfm?fuseaction=userTour.home (last visited Oct. 9, 2009) ("MySpace is a place for friends; MySpace is Your Space; MySpace keeps you connected.").

29. *See* Facebook, http://www.facebook.com/ (last visited Oct. 9, 2009) ("Facebook helps you connect and share with the people in your life.").

30. boyd & Ellison, *supra* note 24.

31. One report notes:

> Facebook members seem to be using Facebook as a surveillance tool for maintaining previous relationships, and as a "social search" tool by which they investigate people they've met offline. There seems to be little "social browsing," or searching for users online initially with the intention of moving that relationship offline.

Cliff Lampe et al., *A Face(book) in the Crowd: Social Searching vs. Social Browsing*, PROC. OF THE 2006 20TH ANNIVERSARY CONF. ON COMPUTER SUPPORTED COOPERATIVE WORK (2006), http://portal.acm.org/citation.cfm?id=1180901.

for social purposes.[32]

The reason for drawing this admittedly imprecise distinction between the two types of service is that these uses or functions will tend to drive differential expectations of privacy, confidentiality, and appropriateness of communications. It is assumed, for example, that those who participate in true professional networking services tend to be more guarded and finite in their engagements. In contrast, those who post or share "what's on [their] mind" on Facebook generally do so with the expectation that they are communicating with a group of friends, an extant social group. Although social networking and social network services function quite similarly, this Article concentrates on the latter group. As such, it ignores social network sites designed solely for healthcare professionals[33] or those that cater to specific diseases or illnesses.[34]

A user of a social network site registers with the service and then creates a profile. This profile functions as the link between the user's real world and virtual world personas. This profile may include a variety of rich media including photographs, videos, and links. Typically, the service will have some kind of search engine that will discover existing real world friends who have a virtual presence in the social network. Usually, a user can opt-out from being so discoverable. Once a user identifies someone with whom they wish to virtually network, they send (e.g., on Facebook) a "friend" request. The network loop is not established until the putative friend accepts that request.[35]

Twitter[36] is similar to the character-limited news feed ("What's on your mind?") popularized by Facebook. But it differs from other social networks because its users are less likely to restrict the viewing of their posts to a restricted group of existing contacts, although that is possible.[37] Users of Twitter "tweet" in bites of up to 140 characters what they are doing or thinking at any particular time. Other Twitter subscribers may then follow these postings. Thus, those who are interesting because they are famous, or famous because they are interesting, have their posts followed by other subscribers, frequently in far larger numbers than Facebook friends. Thus, Twitter shares characteristics with web (particularly blog) sites in that it tends to operate as a broadcast or one-to-many service. As predominantly used, Twitter lacks a key property of other popular social networks in that the publisher of a message typically will not control who

---

32. Lenhart, *supra* note 2, at 6.

33. *See, e.g.*, Sermo, http://www.sermo.com/ (last visited Oct. 10, 2009).

34. *See, e.g.*, PatientsLikeMe, http://www.patientslikeme.com (last visited Oct. 10, 2009); *see* Jeana H. Frost & Michael P. Massagli, *Social Uses of Personal Health Information Within PatientsLikeMe, an Online Patient Community: What Can Happen When Patients Have Access to One Another's Data*, 10 J. MED. INTERNET RES., at e15 (2008), http://www.jmir.org/2008/3/e15/.

35. *See generally* boyd & Ellison, *supra* note 24 (describing social networking sites' procedures for participation).

36. *See* About Twitter, http://twitter.com/about ("Twitter is a real-time information network powered by people all around the world that lets you share and discover what's happening now.").

37. Just as it is possible, but less likely, that a user will open his or her Facebook page to the public.

can see that post (i.e., it is one-directional rather than bi-directional[38]); although it does resemble a service such as Facebook, in that the consumer can choose whether or not to subscribe to posts from that other user.[39]

B. Use, Perceptions, and Expectations

Basic Internet communication tools are either limited in their reach or obvious as to their broadcast nature. Notwithstanding the occasional breakdown when a user ill advisedly clicks "reply to all" or "reply" on a listserv, email is, and is perceived to be, a one-to-one communication. In practice, email may be no more private than sending a postcard through the mail because it could potentially be read by many, but few postcards are read by unintended recipients. At the other extreme, the publisher of content to a web page or a traditional blog should realize that this is a one-to-many broadcast.

In the much-discussed world of Web 2.0, where the creation or sharing of content by users rather than traditional content publishers is emphasized,[40] online search, communication, and networking tools allow those online to apply a virtual overlay to their offline lives. Thus, a user who enters an address into Google Maps creates a representation of that real place. When that user enables location services on a mobile device[41] and allows the online service to share that data with others, the user's real and virtual world locations are overlaid. Similarly, when a user converses on a social network service he or she is mapping his or her virtual conversation to his or her real network of friends and acquaintances. Facebook refers to this as "the digital mapping of people's real-world social connections."[42] However, the potential consequences of such virtual communication are of a different order.

Real world, or offline, communications are beset by inefficiencies and noise

---

38. *See* boyd & Ellison, *supra* note 24.

39. The terrain is further complicated by interactions between these services. For example, Twitter users can link their "tweets" to Facebook so that they are displayed in Facebook as news feeds. *See* Tweeter, Tweeter Is on Facebook, http://www.facebook.com/apps/application.php?id=16268963069 (last visited July 10, 2009).

40. *See* Jessi Hempel, *Web 2.0 Is So Over. Welcome to Web 3.0*, FORTUNE, Jan. 8, 2009, http://money.cnn.com/2009/01/07/technology/hempel_threepointo.fortune/index.htm; *see also* Gunther Eysenbach, *Medicine 2.0: Social Networking, Collaboration, Participation, Apomediation, and Openness*, 10 J. MED. INTERNET RES., at e22 (2008), http://www.jmir.org/2008/3/e22; Benjamin Hughes et al., *Health 2.0 and Medicine 2.0: Tensions and Controversies in the Field*, 10 J. MED. INTERNET RES., at e23 (2008), http://www.jmir.org/2008/3/e23/; Rick McLean et al., *The Effect of Web 2.0 on the Future of Medical Practice and Education: Darwikinian Evolution or Folksonomic Revolution?*, 187 MED J. AUSTL. 174, 174 (2007); Tim O'Reilly, *What Is Web 2.0? Design Patterns and Business Models for the Next Generation of Software*, O'REILLY, Sept. 30, 2005, http://www.oreilly.de/artikel/web20.html.

41. *See, e.g.*, Apple, Phone and iPod Touch: Understanding Location Services, http://support.apple.com/kb/HT1975 (last visited Feb. 8, 2010).

42. Facebook, Press Room, http://www.facebook.com/press.php (last visited Oct. 10, 2009).

that have the effect of limiting the reach of the participants' communications. The context of the listening group[43] will, or should, modulate the content of the conversation. Social network services break this paradigm because they encourage and operationalize the posting of intimate or private moments or thoughts on the user's news feed, wall, or in a tweet. Services such as Facebook confuse the communication model for the user and potentially lead to category breakdown because they offer the opportunity for apparently one-to-one conversations[44] that are nevertheless open to all in a group (a broadcast context).

This initial category breakdown—or state of pseudo-seclusion—is exacerbated in online social networks because the smaller, inefficient, and segregated social categories we tend to have in the real world (relatively distinct categories of intimates, co-employees, co-professionals, etc.) may become blurred when we create larger aggregated friend groups from several categories. For example, a Facebook user's network of friends likely will start with a small number of intimates. As the social network service's tools for finding friends are used,[45] the properties of the friended group may have changed dramatically to include co-workers, employers, or customers.

It may be the case that users of social network sites are "quite oblivious, unconcerned, or just pragmatic about their personal privacy."[46] Equally, such users may be willing to trade their private information knowingly, usually only shared with intimates, in order to increase their number of friends and build new online or offline relationships.[47] In their study of information sharing on Facebook, Gross and Acquisti examined the tenuous application of social network theory[48] to online networks. As they observed, although offline social networks may consist of extremely diverse relationships from intimates to acquaintances, online networks can "reduce these nuanced connections to simplistic binary relations: 'Friend or not.'"[49] Although the context changes as

---

43. For example, an audience of intimates or co-workers around the water-cooler would be a listening group.

44. An example of this would be a wall comment.

45. Examples of friend finding tools include Facebook's ability to allow users to data mine one's Gmail address book or "friending" mere acquaintances who are friends of friends.

46. Ralph Gross & Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks (The Facebook Case)*, (ACM) WORKSHOP IN PRIVACY IN ELECTRONIC SOC'Y 71, § 4 (2005).

47. *See, e.g.*, Catherine Dwyer et al., *Trust and Privacy Concern Within Social Networking Sites: A Comparison of Facebook and MySpace*, AMS. CONF. ON INFO. SYSTEMS 2007 PROC., Paper 339, http://aisel.aisnet.org/amcis2007/339.

48. This sociological construct identifies the properties of social relationships as "nodes" and "ties" and the relative strengths (e.g., weak or strong) of the latter. *See Social Network*, *in* WIKIPEDIA, http://en.wikipedia.org/wiki/Social_network.

49. Gross & Acquisti, *supra* note 46, § 2.1 (quoting d. boyd, *Friendster and Publicly Articulated Social Networking*, *in* 2004 CONF. ON HUM. FACTORS & COMPUTING SYS.) As discussed below, Facebook now permits disaggregation of "friends" into multiple categories that can then be set with different permissions. However, there is no indication yet as to how many

the user moves from offline to online discourse and data sharing, the user may not be fully aware of the category blurring and fail to appropriately modulate the content.

Social network services also impact how users interact with their posted data or content due to a shift from taxonomy, top-down indexing by experts or content owners, to folksonomy (bottom-up indexing or "social tagging" by users).[50] Consider the participant in our water cooler conversation who shows a recent photograph to the other participants. Our participant likely will contextualize the image (e.g., "last weekend-a quiet celebration with friends"). This taxonomy (or metadata) will exclusively index that image for the other participants. Now, consider the same image uploaded to the participant's social network site. Because the site allows tagging of content by other users, folksonomy, the content owner loses exclusive control of the indexing of the image. Now, a "friend" may tag (add metadata to) the image (say, by adding information as to the identity of other participants) or comment on it. Thus, an image that was benign in the water-cooler setting may be re-indexed by other users (e.g., "drunk at medical school reunion;" or "so, that's why you missed work"). As follows from the discussion above, this re-indexing occurs in a context that allows broadcast to a much larger group consisting of multiple offline but aggregated online social categories.

C. Social Network Privacy and Security Settings

Most social network services provide tools for making data or communications less public. Facebook allows users to choose which information to include in their profiles and limit which users can see that information.[51] MySpace and Twitter similarly allow users to control who can see their profile information.[52] Appropriately risk-averse users may also choose to opt out of the popular social network sites and only post on networks restricted to other licensed physicians.[53] Indeed, users with multiple profiles tend to create them on different sites. Of social network site users who have multiple profiles, 25% do so in order to disaggregate their followers, for example by keeping professional

---

users opt to use this feature.

50. *See, e.g.*, Daniel H. Pink, *Folksonomy*, N.Y. TIMES MAG., Dec. 11, 2005, at 69, *available at* http://www.nytimes.com/2005/12/11/magazine/11ideas1-21.html?_r=z; J. Trant, *Studying Social Tagging and Folksonomy: A Review and Framework*, 10 J. DIGITAL INF. (2009); *see also* McLean et al., *supra* note 40, at 175.

51. Facebook, Facebook's Privacy Policy, http://www.facebook.com/policy.php (last visited Dec. 28, 2009).

52. *See* MySpace, About Settings, http://www.myspace.com/Modules/ContentManagement/Pages/page.aspx?placement=privacy_settings, (last visited Oct. 10, 2009); Welcome to Twitter Support!, http://help.twitter.com/portal (last visited Oct. 10, 2009).

53. *See, e.g.*, Sermo, http://www.sermo.com (last visited Dec. 28, 2009). "Sermo uses a proprietary technology to verify physicians' credentials in real-time." Get to Know Sermo, http://www.sermo.com/about/introduction (last visited Feb. 8, 2010).

relationships on one site and personal ones on another.[54]

Popular social network sites offer an array of privacy and security strategies. For example, by using included private modes of communication, users can initiate secure communication without adjusting privacy settings at all. Thus, Facebook, MySpace, and Twitter allow for private messages to be exchanged directly between users,[55] limiting more sensitive conversations to a specific recipient. Similarly, Facebook allows users to exchange real-time instant messages that can only be viewed temporarily,[56] lessening concerns about communication records being used later in a negative manner.

Recently distinguishing itself from competitors, Facebook now permits disaggregation of "friends" into multiple categories that can then be set with different permissions.[57] Utilizing this feature should allow a user to enjoy more relaxed security settings with intimates while benefiting from tightened privacy control for professional contacts.[58] Simply educating users about these settings can radically reduce exposure of private or semi-private information. For example, the authors of the Florida medical student and resident survey discussed below[59] reported that, "telling students to increase their privacy settings on Facebook yielded an 80% reduction in publicly visible accounts."[60]

However, such risk management strategies are seriously under-utilized because so few users change the "open" default privacy and security settings on social network sites.[61] A study conducted by MIT students found that over 70% of the Facebook profiles examined were open to the public.[62] This is an alarming number when considering that a Pew study found that "47% of internet users

---

54. Lenhart, *supra* note 2, at 8.

55. Facebook Help Center: Messages and Inbox, http://www.facebook.com/help/?page=real-time406#!/help.php?page=938 (last visited Feb. 8, 2010); *see also* MySpace, Can You Send Messages to Several Friends at a Time?, http://faq.myspace.com/app/answers/detail/a_id/262/kw/myspace%20mail/c/%20/r_id/ 100061, (last visited Oct. 11, 2009); Twitter Support, http://help.twitter.com/portal, (last visited Oct. 11, 2009).

56. Facebook Help Center: Chat: How to Use the Chat Feature, http://www.facebook.com/help.php?page=824 (follow "How do I delete or look through my chat history? Is it saved permanently?" hyperlink), (last visited Oct. 11, 2009) ("You cannot view older conversations or conversations with friends who are not currently online.").

57. *See also* Posting of Alison Driscoll to Mashable: The Social Media Guide, http://mashable.com/2009/04/28/facebook-privacy-settings/ (Apr. 28, 2009).

58. *See generally* Posting of Marshall Kirkpatrick to ReadWriteWeb, http://www.readwriteweb.com/archives/a_closer_look_at_facebooks_new_privacy_options.php (June 29, 2009, 12:37).

59. *See infra* text accompanying note 267.

60. L.A. Thompson et al., *Author Reply*, J. GEN. INTERNAL MED. 2156, 2156 (2008) (citation omitted).

61. *Compare* Gross & Acquisti, *supra* note 46, § 5, *with* Lenhart, *supra* note 2, at 9 (reporting sixty percent of adult users restrict access to their profiles to friends).

62. Harvey Jones & José Hiram Soltren, *Facebook: Threats to Privacy* 13 (2005), http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall05-papers/facebook.pdf.

look online for information about doctors."[63] Further, the MIT study was conducted by using software to automatically examine the information available in user profiles.[64] Even temporarily unsecured profiles have the potential of being subject to mass data collection, putting users at risk of having their information permanently stored by third-party data aggregators.[65]

Even proper and consistent use of privacy or security settings has some limitations. Needless to say, such privacy and security settings may, as with any other type of online data storage, be defeated by hackers.[66] However, social network sites are not subject to the same comprehensive security requirements as HIPAA mandates for healthcare entities.[67] More importantly, data that is de-identified or rendered pseudonymous may be re-identified if the user has the same profile picture or other demographic data both on one secure and another insecure profile.[68] Users may also defeat the purpose of privacy controls by exercising poor judgment in choosing whom to "friend."[69] For example, a user could have a secured profile but post a comment on another user's public profile that anyone can see.

Ultimately the solution to many but not all of the issues discussed in this article will themselves be technological. Larry Lessig's view of code, or system, architecture holds true here, and suggests that features of the architecture of social network sites will "constrain some behavior by making other behavior possible, or impossible."[70] Changes in the privacy and security settings of Facebook and other social networking sites will likely be the most efficient "regulation" of these issues, certainly more efficient than case-by-case application of the law of boundaries. As the potential for employment or the availability of health insurance are publicly seen as dependent on more responsible online behavior, so the demand for better architecture will increase, as will its utilization, and the spiral will continue until only outlying scenarios

---

63. Susannah Fox & Sydney Jones, *The Social Life of Health Information*, PEW INTERNET & AMERICAN LIFE PROJECT 35 (2009), http://www.pewinternet.org/~/media//Files/Reports/2009/PIP_Health_2009.pdf.

64. Jones & Soltren, *supra* note 62, at 11.

65. *Id.*

66. *See, e.g.*, Claire Cain Miller & Brad Stone, *Twitter Hack Raises Flags on Security*, N.Y. TIMES, July 15, 2009, http://www.nytimes.com/2009/07/16/technology/internet/16twitter.html?ref=technology; Posting of Chris Dannen to Fast Company.com, http://www.fastcompany.com/blog/chris-dannen/techwatch/10-questions-answered-facebook-attacks (May 15, 2009 12:30). Hacking of social network sites (or even government surveillance of same) is outside the terms of reference of this article. In such cases statutory protections involving criminal and civil liability may apply, for example, under the Electronic Communications Privacy Act of 1986. *See* 18 U.S.C. §§ 2510-2522 (2006).

67. *See* 45 C.F.R. §§ 160, 162, 164 (2009).

68. Gross & Acquisti, *supra* note 46, § 4.2.

69. *See* Jones & Soltren, *supra* note 62, at 20 (explaining that their study found 28.7% of Facebook users "friend strangers on occasion").

70. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 89 (1999).

remain.

In parallel to architectural evolution facilitated by code innovation and prompted by market pressures from competitors or consumers, social network services may find themselves subject to low levels of what Anita Allen has, in analogous situations, termed state "coercion."[71] Thus, the FTC could exert marginal coercion by opening an investigation into social networking site defaults or, as is happening in Canada, apply additional yet still minimal coercion by demanding specific changes to the sites' settings.[72]

Whatever the drivers, changes in architecture clearly are foreseeable but are likely to be incremental. The fact that regulation of the physician-patient relationship and the protection of patient information are so entrenched in our health law models (common law, statute, constitutional law, command-control, ethical codes, etc.) makes it unlikely that courts and regulators will wait too long for better "code."

II. THE LEGAL (AND NOT SO LEGAL) FRAMEWORK

There are a multitude of emerging legal issues surrounding social network sites and the vast amounts of data contained on them. For example, social network data is of interest to anti-terrorist agencies in much the same way as email and telephone archives;[73] an Australian court allowed lawyers to serve notice of a default judgment via Facebook on two borrowers who had defaulted on a loan;[74] and social network postings have come under scrutiny in cases of jurors apparently researching and discussing cases on Twitter and Facebook.[75]

---

71. *See* Anita L. Allen, *Unpopular Privacy: The Case for Government Mandates*, 32 OKLA. CITY U. L. REV. 87, 96-98 (2007) (discussing FTC regulation of telemarketing calls through the National Do Not Call Registry).

72. *See, e.g.*, Press Release, Office of the Privacy Comm'r of Can., Facebook Needs to Improve Privacy Practices, Investigation Finds (July 16, 2009), *available at* http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_e.cfm. Facebook responded with proposed changes to its policies and code; *see* Posting of Claire Cain Miller to Bits, http://bits.blogs.nytimes.com/2009/08/27/facebook-moves-to-improve-privacy-and-transparency (Aug. 27, 2009, 13:52 EST).

73. *See, e.g.*, *Social Network Sites 'Monitored'*, BBC NEWS ONLINE, Mar. 25 2009, http://news.bbc.co.uk/2/hi/uk_news/politics/7962631.stm (discussing telecommunications data retention under European Union directive).

74. Noel Towell, *Lawyers to Serve Notices on Facebook*, SYDNEY MORNING HERALD, Dec. 16, 2008, http://www.smh.com.au/news/technology/biztech/lawyers-to-serve-notices-on-facebook/2008/12/16/1229189579001.html.

75. John Schwartz, *As Jurors Turn to Web, Mistrials Are Popping Up*, N.Y. TIMES, Mar. 18, 2009, at A1, *available at* http://www.nytimes.com/2009/03/18/us/18juries.html; Scott Michels, *Cases Challenged over 'Tweeting' Jurors: Lawyers Say They Will Appeal Verdicts After Jurors Comment on Facebook, Twitter*, ABC NEWS, Mar. 17, 2009, http://abcnews.go.com/Technology/Story?id=7095018&page=1; *Facebook, Twitter Throw US Legal System into Disarray*, ABC NEWS (Australia), Mar. 18, 2009, http://www.abc.net.au/news/stories/2009/03/18/2520009.htm; *see also* Kate Moser, *Court Lays Down Law on Jury Internet Use*, RECORDER, Sept. 9, 2009,

Even the status of the very media and data uploaded to social network sites is somewhat uncertain. For example, in February 2009 Facebook changed its terms of use, and for the first time suggested that it had persisting rights in some user-submitted content.[76] Although Facebook changed back to its earlier terms of use,[77] even under the current terms of use some user-uploaded content may persist (when shared with other subscribers or in back-ups) even when deleted by the user.[78]

This Article concentrates on just one risk-laden aspect of the use of such networks—the potential for category breakdown between social and healthcare professional uses and its implication for social and professional data. Given that we are concerned primarily with private actors (users of social network sites and those who would view, process, or aggregate user data), the reflexive response is to turn to the Law of Boundaries as the exclusive legal model. Within this concept, the common law of privacy governs social boundaries, while a more complex set of common law, ethical, and regulatory provisions governs professional boundaries. As will be seen, this intuitive response translates into an accurate picture of both the legal structures most likely to be applicable and the legal protection choices of those dissatisfied with treatment of their social network data. But the Law of Boundaries does not provide the exclusive options for dealing with category breakdown. Other options are present that may prove more or less attractive as these (and related) online interactions develop.

---

http://www.law.com/flat/ltn/ 1202433656715.html (describing proposed San Francisco Superior Court rule on subject).

76. Brian Stelter, *Facebook's Users Ask Who Owns Information*, N.Y. TIMES, Feb. 17, 2009, at B3, *available at* http://www.nytimes.com/2009/02/17/technology/internet/17facebook.html.

77. *Facebook Backs Down, Reverses on User Information Policy*, CNN.COM, Feb. 18, 2009, http://www.cnn.com/2009/TECH/02/18/facebook.reversal/index.html.

78. Facebook, *Statement of Rights and Responsibilities*, http://www.facebook.com/terms.php.

> 2. Sharing Your Content and Information
>
> You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings. In addition:
>
> > 1. For content that is covered by intellectual property rights, like photos and videos ("IP content"), you specifically give us the following permission, subject to your privacy and application settings: you grant us a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that you post on or in connection with Facebook ("IP License"). This IP License ends when you delete your IP content or your account unless your content has been shared with others, and they have not deleted it.
> >
> > 2. When you delete IP content, it is deleted in a manner similar to emptying the recycle bin on a computer. However, you understand that removed content may persist in backup copies for a reasonable period of time (but will not be available to others).

A. Options: Property, Liability, Inalienability, and Soft Law

The conventional wisdom is that interests in personal health data are protected by liability not property rules. Thus, health information is not directly protected as, for example, an intellectual property system might wall-off some scientific data. Rather, the law of boundaries (HIPAA included) places behavioral limits on those who would obtain or who are entrusted with health information.[79] Even some data protection rules that appear to flirt with property, such as rules that exclude regulation of de-identified personal health data,[80] are better understood as liability rules that provide safe harbors for data custodians who behave in certain ways.[81]

There are compelling arguments that property rules are underused in protecting personally identifiable information.[82] However, of more practical interest in the context of this article is the opening of a "third front," in addition to property or liability constructs: the option of protecting personal information on social networks with some form of inalienability rule.[83]

Stated broadly inalienability denotes non-transferability of an entitlement (herein personally identifiable data) even with (the data subject's) consent. Here Margaret Jane Radin's unpacking of inalienability is helpful as is her identification of "market-inalienability" that "places some things outside the marketplace but not outside the realm of social intercourse."[84] With a targeted inalienability regime it is possible to avoid the on (property) and sometimes off (liability) approaches to tradability in personal information. Specifically, we can impose bright line rules that target specific would-be uses or users of the data.

Recent developments in health information regulation suggest a growing interest in this targeted approach. For example, the recently-enacted federal Health Information Technology for Economic and Clinical Health Act (HITECH)[85] provides for market inalienability regarding information contained

---

79. *See generally* NICOLAS P. TERRY, LEGAL ISSUES RELATED TO DATA ACCESS, POOLING, AND USE IN HEALTHCARE DATA IN PUBLIC GOOD OR PRIVATE PROPERTY? Ch. 4 (National Institutes of Health, forthcoming 2010).

80. *See, e.g.*, 45 C.F.R. § 160.103 (2009) (defining protected health information as that which is "individually identifiable").

81. *See, e.g., id.* § 164.514(e)(3)(i) (de-identifying the data or complying with "limited data set" rules).

82. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000) (dissecting the inapplicability of property as itself conclusory of the property and liberty rhetoric of those who would trade in the data of others).

83. *See generally* Guido Calabresi & A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 HARV. L. REV. 1089 (1972); Margaret Jane Radin, *Market-Inalienability*, 100 HARV. L. REV. 1849 (1987); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055 (2004).

84. Radin, *supra* note 83, at 1853.

85. *See infra* note 240 and accompanying text.

in a patient's electronic medical record.[86] Similarly, a handful of states have targeted specific uses of prescribing information collected by data aggregators on behalf of pharmaceutical manufacturers desirous of more efficient marketing of their drugs to physicians.[87] The data aggregators initially were successful in arguing that such statutes violated their commercial speech rights.[88] However, the First Circuit recently validated the regulatory approach when it characterized the limited target prohibition in the New Hampshire statute as restricting conduct, not speech.[89]

Moving forward, inalienability models are useful if we end up concluding that we want to wall-off the social network playground in a less extreme or more targeted manner than by using the Law of Boundaries. Inalienability rules could prohibit the acquisition of some online information by identified cohorts (for example, health insurers) or particular uses of such data (for example, employment-related decisions).[90]

Finally, in examining the palette of options for dealing with the interaction of social network information and the physician-patient relationship, we must consider soft law models of regulation. Soft law is notoriously difficult to define.[91] Previously discussed architectural or code approaches to data protection driven by standards bodies or industry associations likely would qualify for the soft law description. But in the present context the most important sources of non-legal, soft regulation are professional ethics codes; provisions of which will inform the discussion that follows.

Inalienability rules and soft law may not operate in series with liability rules (such as the Law of Boundaries). Just as common law rules tend to exhibit cycles of on/off switches punctuated by exceptionalism,[92] so highly targeted inalienability or soft law rules may occupy a transitional space while courts determine longer-term entitlements. Equally, narrowly constructed inalienability rules that are consistent with emerging architectural and soft law constructs in, say, being increasingly protective of social network data likely will propel the

---

86. Health Information Technology for Economic and Clinical Health Act, 42 U.S.C.A. § 17935(d) (effective Feb. 17, 2010).

87. *See, e.g.*, N.H. REV. STAT. ANN. § 318:47-f (2009); ME. REV. STAT. ANN. 22 § 1711-E (Supp. 2009).

88. *See, e.g.*, IMS Health, Inc. v. Ayotte, 490 F. Supp. 2d 163 (D.N.H. 2007), *rev'd and vacated*, 550 F.3d 42 (1st Cir. 2008); IMS Health Corp. v. Rowe, 532 F. Supp. 2d 153 (D. Me. 2008).

89. *See* IMS Health Inc. v. Ayotte, 550 F.3d 42, 52 (1st Cir. 2008), *cert. denied*, 129 S. Ct. 2864 (2009).

90. *See, e.g.*, Dina Epstein, *Have I Been Googled?: Character and Fitness in the Age of Google, Facebook, and YouTube*, 21 GEO. J. LEGAL ETHICS 715, 727 (2008) (arguing that the ABA should outlaw consideration of social network data for character and fitness determinations).

91. *See, e.g.*, Anna di Robilant, *Genealogies of Soft Law*, 54 AM. J. COMP. L. 499, 500-01 (2006).

92. *See* Nicolas P. Terry, *Collapsing Torts*, 25 CONN. L. REV. 717, 736-38 (1993), building on EDWARD H. LEVI, AN INTRODUCTION TO LEGAL REASONING 8-27 (1949).

courts utilizing conventional boundary law mechanisms towards a similarly protective stance.

B. The Law of Boundaries: Privacy Torts and Breach of Confidence

The Restatement's black-letter law of privacy fails to provide any general or comprehensive right of privacy. Rather, the common law of privacy consists of a group of nominate, discrete, and limited tort causes of action, somewhat unconvincingly bundled together in the RESTATEMENT (SECOND) OF TORTS.[93] Most jurisdictions recognize four causes of action for invasion of privacy: intrusion, public disclosure (or publicity) of private facts, false light, and appropriation (or exploitation) of another's name.[94] In the context of this article the intrusion and publicity torts are of most importance.[95]

Both the intrusion and publicity torts are collection-centric. That is, they provide for legal disincentives to the collection or exploitation of private information. The intrusion tort focuses on the manner of acquisition of the information while the publicity tort focuses on the content of the information.[96] In contrast, the action for breach of confidence recognized in most jurisdictions[97] is disclosure-centric and focuses on the underlying relational source of the information.[98]

Today courts tend to view the privacy tort as one of public disclosure of embarrassing facts.[99] As such it appears to have more in common with the

---

93. RESTATEMENT (SECOND) OF TORTS §§ 652A-652I (1977); *see, e.g.*, Reid v. Pierce County, 961 P.2d 333, 339 (Wash. 1998) (en banc) (adopting § 652).

94. *See Reid*, 961 P.2d at 338-39; Estate of Berthiaume v. Pratt, 365 A.2d 792, 795 (Me. 1976); Loft v. Fuller, 408 So. 2d 619, 622 (Fla. Dist. Ct. App. 1981).

95. Of least importance in the context of this article are the "appropriation" (§ 652C) and "false light" torts. RESTATEMENT (SECOND) OF TORTS §§ 652C, 652E. Additionally, not all jurisdictions recognize the "false light" action primarily because it is somewhat duplicative of the tort of defamation. Jews for Jesus, Inc. v. Rapp, 997 So. 2d 1098, 1113 (Fla. 2008). *But see* Meyerkord v. Zipatoni Co., 276 S.W.3d 319, 326 (Mo. Ct. App. 2008) (joining majority of jurisdictions in recognizing "false light" claim and navigating overlap with defamation). Although not of particular relevance to the issues discussed herein, it is likely we will see considerable appropriation litigation regarding social network sites. *See, e.g.*, Web 2.0 Convergence, http://www.digitalcommunitiesblogs.com/web_20_convergence/2009/06/social-media-fraud-on-the-incr.php (June 8, 2009 14:32) (discussing impersonation of media and athletic personalities in twitter feeds).

96. *See* Alan B. Vickery, Note, *Breach of Confidence: An Emerging Tort*, 82 COLUM. L. REV. 1426, 1441 (1982) (making a content-source distinction).

97. *Cf.* Meade v. Orthopedic Assocs. of Windham County, No. CV064005043, 2007 Conn. Super. LEXIS 3424, at *14 (Conn. Super. Ct. Dec. 27, 2007) (declining to recognize cause of action for breach of confidence).

98. *See, e.g.*, Burger v. Blair Med. Assocs., Inc., 964 A.2d 374, 378 (Pa. 2009); McCormick v. England, 494 S.E.2d 431, 435 (S.C. Ct. App. 1997).

99. Stratton v. Krywko, No. 248669, 2005 Mich. App. LEXIS 23, at *11 (Mich. Ct. App. Jan.

disclosure-centric confidentiality duty than the collection-centric intrusion tort. But it remains collection-centric side of the line because of its predicate that the defendant acquired private, embarrassing facts about the plaintiff before disclosure. In contrast, the confidentiality predicate is not one of acquisition by the defendant—rather, the plaintiff delivered the (typically) private information to the defendant in the context of a preexisting, fiduciary relationship.

Based as they are on underlying, preexisting relationships, breach of confidence actions are heavily dependent on context and the properties of the underlying relationship. In the context of the physician-patient relationship and the data entrusted in that context, the breach of confidence actions discussed below are variously based on responsibilities imposed by licensing statutes, the physician's evidentiary privilege, common law principles of trust, the Hippocratic Oath, and general principles of medical ethics.[100]

1. Intrusion upon Seclusion.—The RESTATEMENT (SECOND) describes the intrusion upon seclusion tort as follows: "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[101] Today, courts require the satisfaction of four elements: (1) an unauthorized intrusion or prying into plaintiff's seclusion; (2) the intrusion is highly offensive or objectionable to a reasonable person; (3) the matter upon which the intrusion occurs must be private; and (4) the intrusion causes anguish and suffering.[102]

The intrusion tort originally required a literal, physical intrusion; this is no longer the case. Courts now tend to look less at the physicality of the defendant's action and more at the level of its offensiveness.[103] The foundation of the action

---

6, 2005).

100. Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580, 590-91 (D.C. 1985).

101. RESTATEMENT (SECOND) OF TORTS § 652B (1966); *see also id.* § 652B cmts. a, b:

> a. The form of invasion of privacy covered by this Section does not depend upon any publicity given to the person whose interest is invaded or to his affairs. It consists solely of an intentional interference with his interest in solitude or seclusion, either as to his person or as to his private affairs or concerns, of a kind that would be highly offensive to a reasonable man.
>
> b. The invasion may be by . . . . some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account . . . .

102. *See, e.g.*, Lovgren v. Citizens First Nat'l Bank of Princeton, 534 N.E.2d 987, 989 (Ill. 1989) (recognizing requirement that intrusion must be "highly" offensive); Schmidt v. Ameritech Ill., 768 N.E.2d 303, 311 (Ill. App. Ct. 2002); *see also Vassiliades*, 492 A.2d at 588 (requiring showing that intrusion be "highly offensive"); Melvin v. Burling, 490 N.E.2d 1011, 1013-14 (Ill. App. Ct. 1986).

103. *See, e.g.*, Bonanno v. Dan Perkins Chevrolet, No. CV 99066602, 2000 Conn. Super. LEXIS 287, at *4-5 (Conn. Super. Ct. Feb. 4, 2000). *See generally* Goodrich v. Waterbury Republican-Am., Inc., 448 A.2d 1317 (Conn. 1982); Johns v. Firstar Bank, No. 2004-CA-001558-

remains an "intentional and unwarranted acquisition by the defendant."[104]

A "wrongful intrusion may occur in a public place, so long as the thing into which there is intrusion or prying is entitled to be private."[105] "However, generally, the observation of another person's activities, when that other person is exposed to the public view, is not actionable. . . ."[106] Thus, training a surveillance camera on the outside of a house likely will not be an intrusion.[107] However, observing people through holes poked in the ceiling of a restroom,[108] or by use of a camera installed in a medical examination room,[109] clearly satisfy the element.

As the courts' understanding of an actionable intrusion has become more existential, their approach has become more nuanced. In the words of one court: "Assuming that the matter is entitled to be private, then the court will consider two primary factors in determining whether an intrusion is actionable: (1) the means used, and (2) the defendant's purpose for obtaining the information."[110] In general, contrasting sharply with other boundary torts, "[i]ntrusion into solitude appears to be based on the manner in which a defendant obtains information, and not what a defendant later does with the information."[111]

2. Public Disclosure of Private Facts.—The publicity tort, targeting those who give "publicity to a matter concerning the private life"[112] of the plaintiff, applies to "[o]ne who gives publicity to a matter concerning the private life of another"[113] if the data "(a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."[114] Modern courts state a granular version of the doctrine as requiring:

> (1) the fact or facts disclosed must be private in nature; (2) the disclosure must be made to the public; (3) the disclosure must be one which would be highly offensive to a reasonable person; (4) the fact or facts disclosed cannot be of legitimate concern to the public; and (5) the defendant acted with reckless disregard of the private nature of the fact or facts disclosed.[115]

A key distinction between the intrusion and publicity causes of action is that

---

MR, 2006 Ky. App. LEXIS 85, at *7-9 (Ky. Ct. App. Mar. 24, 2006).

104. Burger v. Blair Med. Assocs., Inc., 964 A.2d 374, 379 (Pa. 2009).

105. Martin v. Patterson, 975 So. 2d 984, 994 (Ala. Civ. App. 2007) (citations omitted).

106. Johnson v. Stewart, 854 So. 2d 544, 549 (Ala. 2002) (citing I.C.U. Investigations, Inc. v. Jones, 780 So. 2d 685 (Ala. 2000)).

107. Schiller v. Mitchell, 828 N.E.2d 323, 327-29 (Ill. App. Ct. 2005).

108. *See* Benitez v. KFC Nat'l Mgmt. Co., 714 N.E.2d 1002, 1033-34 (Ill. App. Ct. 1999).

109. Acuff v. IBP, Inc., 77 F. Supp. 2d 914, 919-21 (C.D. Ill. 1999).

110. *Martin*, 975 So. 2d at 994 (citations omitted).

111. Fernandez-Wells v. Beauvais, 983 P.2d 1006, 1010 (N.M. Ct. App. 1999).

112. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

113. *Id.*

114. *Id.*

115. Robert C. Ozer, P.C. v. Borquez, 940 P.2d 371, 379 (Colo. 1997).

although the former "requires *no* showing of publication or publicity,"[116] the publicity action rotates around the *public disclosure* of private facts.[117]

3. Breach of Confidence.—The privacy torts closely resemble intentional torts such as outrage,[118] in that they rotate around intentional interferences[119] that are "highly offensive to a reasonable person."[120] In contrast, the breach of confidence tort is essentially a strict liability action,[121] as befits a tort claim that has its roots in implied contract and fiduciary duties.[122]

Confidentiality, or rather the tort of breach of confidence, is disclosure-centric. The breach of confidence tort applies only to those who have been entrusted with information in confidence.[123] Accordingly:

> The [fiduciary or confidential] relationship arises when one person reposes special trust and confidence in another person and that other person—the fiduciary—undertakes to assume responsibility for the affairs of the other party. The person upon whom the trust and confidence is imposed is under a duty to act for and to give advice for the benefit of the other person on matters within the scope of the relationship. Fiduciary duties are the highest standard of duty imposed by law.[124]

It follows that "only one who holds information in confidence can be charged with a breach of confidence,"[125] while "an act [that] qualifies as a tortious invasion of privacy, it theoretically could be committed by anyone."[126] The converse is true; if information that is not secret or private is entrusted in

---

116. Corcoran v. Sw. Bell Tel. Co., 572 S.W.2d 212, 215 (Mo. Ct. App. 1978); *see also* Lovgren v. Citizens First Nat'l Bank, 534 N.E.2d 987, 989 (Ill. 1989) ("The basis of the tort is not publication or publicity. Rather, the core of this tort is the offensive prying into the private domain of another.").

117. *See, e.g.*, Tureen v. Equifax, Inc., 571 F.2d 411, 419 (8th Cir. 1978) (requiring "disclosure to the general public or likely to reach the general public").

118. RESTATEMENT (SECOND) OF TORTS § 46 (1965).

119. *See, e.g.*, Meyerkord v. Zipatoni Co., 276 S.W.3d 319, 326 (Mo. Ct. App. 2008) (requiring plaintiff allege that defendant acted with "knowledge of or with reckless disregard").

120. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

121. *See* Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580, 591 (D.C. 1985).

122. *See generally* Biddle v. Warren Gen. Hosp., 715 N.E.2d 518, 523 (Ohio 1999) (noting that the physician-patient relationship includes a fiduciary character component); Overstreet v. TRW Commercial Steering Div., 256 S.W.3d 626, 631-32 (Tenn. 2008) (discussing covenants of confidentiality for contracts implied in fact and contracts implied in law); McCormick v. England, 494 S.E.2d 431, 434 (S.C. Ct. App. 1997) (recognizing modern tort law basis of action).

123. *See, e.g.*, Johns v. Firstar Bank, No. 2004-CA-001558MR, 2006 Ky. App. LEXIS 85, at *8-9 (Ky. Ct. App. Mar. 24, 2006) (finding that privacy torts are not applicable to a case where plaintiff disclosed information to defendant; any action would have to lie in breach of confidence).

124. *Overstreet*, 256 S.W.3d at 641-42 (Koch, J., concurring) (internal citations omitted).

125. Humphers v. First Interstate Bank, 696 P.2d 527, 530 (Or. 1985) (en banc).

126. *Id.*

confidence, its subsequent disclosure may be actionable.[127] Although there can be overlap, "neither of the torts of invasion of privacy nor breach of confidentiality is entirely subsumed within the other."[128]

The breach of confidence tort not only is a stricter form of liability than privacy theories, but also eschews the defensive arguments available in the latter. For example, "[a] defendant is not released from an obligation of confidence merely because the information learned constitutes a matter of legitimate public interest."[129]

C. Privacy Expectations and Social Networks

Obviously privacy policies do not protect social network subscribers from legal process.[130] Increasingly, and as happened with email, social network subscribers' private profile pages are drawn into public processes through subpoena or discovery.[131] For example, there have been media reports of prosecutors using photographs posted on defendants' social network sites to bolster their arguments in sentencing hearings.[132] Indeed, a growing number of cases involve discovery or related procedural requests by defendants.[133] Representative fact-patterns include workplace sexual harassment claims, where the defendant argues that the plaintiff consensually engaged in similar behaviors online,[134] and any number of cases where the defense seeks to make an issue out of the social network subscriber's emotional state.[135]

---

127. *See id.* at 528.

128. Burger v. Blair Med. Assocs., Inc., 964 A.2d 374, 381 (Pa. 2009).

129. Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580, 591 (D.C. 1985) (citing Vickery, *supra* note 96, at 1468).

130. *See, e.g.*, Facebook's Privacy Policy, http://www.facebook.com/policy.php (last visited Dec. 30, 2009) ("We may disclose information pursuant to subpoenas, court orders . . . if we have a good faith belief that the response is required by law.").

131. *See, e.g.*, Ronald J. Levine & Susan L. Swatski-Lebson, *Are Social Networking Sites Discoverable?*, PRODUCT LIABILITY L. & STRATEGY, Nov. 13, 2008, *available at* http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1202425974937.

132. *See* Associated Press, *Facebook Evidence Sends Unrepentant Partier to Prison*, FOX NEWS.COM, July 21, 2008, http://www.foxnews.com/story/0,2933,386241,00.html.

133. *See generally* Carole Levitt & Mark Rosch, *How Lawyers Can Mine a Social Network for Personal Information*, 16 NEV. LAW. 12 (2008).

134. *See, e.g.*, Mackelprang v. Fid. Nat'l Title Agency of Nev., Inc., No. 2:06-cv-00788-JCM-GWF, 2007 U.S. Dist. LEXIS 2379, at *8-9 (D. Nev. Jan. 9, 2007).

135. *See, e.g.*, Mary Pat Gallagher, *MySpace, Facebook Pages Called Key to Dispute Over Insurance Coverage for Eating Disorders*, 191 N.J.L.J. 309, Feb. 1, 2008, *available at* http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=900005559933 (discussing *Beye v. Horizon* and *Foley v. Horizon*, in which defendant's health insurer argued that access to social network pages could assist in a defense for denial of coverage for anorexia or bulimia because conditions were emotionally rather than biologically caused); Henry Gottlieb, *MySpace, Facebook Privacy Limits Tested in Emotional Distress Suit*, 188 N.J.L.J. 845, June 14, 2007, *available at*

In such cases the exact legal status of social network content vis-à-vis user expectations tends to be obscured by proceedings that depend in large part on highly individualized facts and trial court discretion. Only occasionally have courts dealt directly with a social network user's expectations of those who can see their posts, or the more complex legal question of the user's privacy expectations.

A.B. v. State[136] concerned a juvenile who posted a vulgar tirade against her ex-middle school principal on a MySpace page. That page was on a profile falsified as the principal's but actually created by one of the defendant's friends.[137] A total of twenty-six friends including the defendant were given access to the fake profile.[138] At trial the defendant was adjudicated a delinquent child on the basis that, if she had been an adult at the time of the crime, she would have committed the statutory offense of harassment.[139] The requisite intent for the harassment offense in question included "a subjective expectation that the offending conduct will likely come to the attention of the person targeted for the harassment."[140] Given the sparse record, the prosecution's reasonable doubt burden, and a lack of any independent evidence as to the workings of the social network site, the court reversed the adjudication.[141] Specifically, the court determined that there was no probative evidence that the defendant, who posted to a limited group of friends rather than the public, had the requisite expectation that the act would come to the principal's intention.[142]

In *Moreno v. Hanford Sentinel, Inc.*,[143] a college student posted comments critical of her hometown on her MySpace site. Although she removed the posting six days later, the post had already been copied to her hometown's newspaper for republication.[144] She sued the newspaper and her high school principal who had transmitted the posting to a reporter for, inter alia, breach of privacy.[145] Citing *Hill v. National Collegiate Athletic Ass'n*,[146] the Supreme Court of California's most recent guide, the court noted that such a claim "is not 'so much one of total secrecy as it is of the right to *define* one's circle of

---

http://www.law.com/jsp/LawArticleFriendly-jsp?id (discussing *T.V. v. Union Township Board of Education*, defendant school district sought access to social networks pages to potentially challenge plaintiffs credibility in an action for emotional injuries).

136. 885 N.E.2d 1223 (Ind. 2008).

137. *Id.* at 1225.

138. *Id.*

139. *Id.* at 1223-25.

140. *Id.* at 1226.

141. *Id.* at 1228.

142. *Id.* at 1227-28. The court seemed less sure about how to deal with another posting by the defendant on a different, public *MySpace* profile page, but ultimately found the evidence wanting as to intent. *Id.*

143. 91 Cal. Rptr. 3d 858 (Ct. App. 2009).

144. *Id.* at 861.

145. *Id.*

146. 865 P.2d 633 (Cal. 1994).

intimacy—to choose who shall see beneath the quotidian mask.'"[147] The *Moreno* court concluded:

> [The plaintiff] publicized her opinions . . . by posting . . . on myspace.com, a hugely popular internet site. [Her] affirmative act made her article available to any person with a computer and thus opened it to the public eye. Under these circumstances, no reasonable person would have had an expectation of privacy regarding the published material.[148]

The opinion does not state whether the plaintiff had set her MySpace privacy settings to restrict access to her site to her approved "friends." As it stands, the opinion seems to suggest that simply posting to a social network site defeats the expectation of privacy; a position that is challenged below.[149]

D. Privacy and Confidentiality in Healthcare

The privacy and confidentiality rules applied to healthcare providers and to some patient information are both more complex and more granular. At common law, the collection-centric privacy tort is represented by a relatively small collection of cases that suggest healthcare provider liability will be restricted to a narrow range of outlying fact situations. Such a state is unsurprising given that the privacy torts lack any unifying concept and have failed to develop robust, plaintiff-friendly doctrine.

Consider, for example, the classic case of *Knight v. Penobscot Bay Medical Center*.[150] A nurse's husband arrived at a hospital to pick her up.[151] "To give [him] something interesting to do while he" waited, the husband was gowned and permitted to observe a stranger's labor and delivery.[152] Notwithstanding the rather obvious nature of this intrusion, the plaintiff's cause of action failed because there was no evidence that the nurse's husband had *intended* the intrusion into the patient's seclusion.[153]

---

147. *Moreno*, 91 Cal. Rptr. 3d at 863 (quoting M.G. v. Time Warner, Inc., 107 Cal. Rptr. 2d 504, 511 (Ct. App. 2001)). *Hill* also analyzed the privacy tort rights as follows:

> Each of the four categories of common law invasion of privacy identifies a distinct interest associated with an individual's control of the process or products of his or her personal life. To the extent there is a common denominator among them, it appears to be improper interference (usually by means of observation or communication) with aspects of life consigned to the realm of the "personal and confidential" by strong and widely shared social norms.

Hill, 865 P.2d at 647.

148. *Moreno*, 91 Cal. Rptr. 3d at 862.

149. *See* text accompanying *infra* notes 323-29.

150. 420 A.2d 915 (Me. 1980).

151. *Id.* at 916-17.

152. *Id.* at 917.

153. *Id.* at 918; *see also* Fisher v. Dep't of Health, 106 P.3d 836, 840 (Wash. Ct. App. 2005) (requiring a "deliberate intrusion"); Kindschi v. City of Meriden, No. CV064022391, 2006 Conn.

Similar limitations that are instructive on the application of the privacy torts to social network scenarios derive from the torts' offensiveness and privacy expectation limitations. Take, for example, *Adamski v. Johnson*,[154] a case that involved intrusion and publicity allegations by the plaintiff against her employer. Plaintiff provided her employer with notice that she would be undergoing surgery, but when asked she refused to supply additional information about the surgery.[155] Allegedly, her supervisor applied pressure to her co-employees and acquired that information.[156] The defendants' apparently intentional conduct notwithstanding, the court granted defendants' demurrer.[157] First, the court did not view the disclosed information regarding the nature of the surgery as either an intrusion or public disclosure of private facts that could be "'highly offensive'" to a reasonable person.[158] Second, the plaintiff's inchoate allegation that her supervisor relayed the information to others was dismissed on the basis that it did not allege facts to suggest that the disclosure went beyond a single person or small group of persons.[159] Third, the plaintiff's own disclosure of the nature of the surgery to a small group of co-workers reinforced the defense position that the intrusion was not offensive and rendered the publicity claim untenable by eliminating her expectation of privacy.[160]

Notwithstanding these limitations inherent in the common law doctrines, there is a considerable body of case law that applies privacy doctrine with some rigor to medical fact patterns and suggests some legal jeopardy for medical professionals posting or micro-blogging information about their patients. As noted as early as 1942 by the Supreme Court of Missouri, "if there is any right of privacy at all, it should include the right to obtain medical treatment at home or in a hospital for an individual personal condition (at least if it is not contagious or dangerous to others) without personal publicity."[161] As more recently stated by a district court in Illinois, "[t]here are few things in life that are more private than medical treatments and/or examinations."[162]

1. Intrusion Actions.—Estate of Berthiaume v. Pratt concerned two series of photographs taken of a patient suffering from cancer of the larynx.[163] The first

---

Super. LEXIS 3666, at *8-9 (Conn. Super. Ct. Nov. 27, 2006) (requiring an intentional invasion upon the plaintiff's privacy).

154. 80 Pa. D. & C.4th 69 (Comm. Pl. 2006).

155. *Id.* at 70-71.

156. *Id.* at 71.

157. *Id.* at 78.

158. *Id.* at 74.

159. *Id.* at 76.

160. *Id.* at 77; *see also* Fletcher v. Price Chopper Foods of Trumann, Inc., 220 F.3d 871, 878 (8th Cir. 2000) (holding that plaintiff lost expectation of privacy when she shared information about a staph infection with co-workers).

161. Barber v. Time, Inc., 159 S.W.2d 291, 295 (Mo. 1942).

162. Acuff v. IBP, Inc., 77 F. Supp. 2d 914, 924 (C.D. Ill. 1999).

163. 365 A.2d 792, 793 (Me. 1976).

series was taken during the patient's treatment and apparently with his consent.[164] A second series was taken as the patient was dying and there was evidence that the patient objected to the taking of this second set of photographs.[165] The court reversed the defendant's directed verdict and held that this intrusion claim should have been submitted to the jury.[166] Although the court recognized "the benefit to the science of medicine which comes from the making of photographs of the treatment and of medical abnormalities found in patients,"[167] this could not be done without the subject's consent.[168]

Stratton v. Krywko concerned a plaintiff involved in an automobile accident.[169] She was taking Prozac and on the night of the accident consumed alcohol and marijuana.[170] With the consent of emergency services and the local hospital, a documentary crew was riding with the paramedics who treated the patient at the scene of the accident and transported her to the emergency room.[171] Plaintiff refused to sign any consent to the filming.[172] In subsequent broadcasts plaintiff's face was digitally obscured.[173] However, she was referred to by her first name and her name and address were visible on a report shown in the video.[174] A physician could be heard referring to her as "[n]o allergies, on Prozac."[175] Given that "defendants filmed plaintiff in the emergency room after she was presented with and explicitly *refused* to sign the informed consent release,"[176] the court held that her intrusion allegation should have been presented to the jury.[177]

Both *Berthiaume* and *Stratton* reaffirm the collection-centric nature of the intrusion action. However, both cases concern the judicial protection of overtly physical spaces and tell us little about the resolution of potential claims involving intrusion into a pseudo-secluded space such as a Facebook profile.

2. Publicity Actions.—Whether information is private depends in part on the type of information and the extent that the subject keeps the information from the public. Thus, "[s]exual relations . . . are normally entirely private matters, as are . . . many unpleasant or disgraceful or humiliating illnesses, most intimate personal letters, [and] most details of a man's life in his home."[178] Indeed,

---

164. *Id.*
165. *Id.*
166. *Id.* at 795.
167. *Id.* at 796.
168. *Id.* at 796-97.
169. No. 248669, 2005 Mich. App. LEXIS 23, at *1-2 (Mich. Ct. App. Jan. 6, 2005).
170. *Id.*
171. *Id.* at *3.
172. *Id.*
173. *Id.* at *3-4.
174. *Id.*
175. *Id.*
176. *Id.* at *22.
177. *Id.*; *see also* Miller v. Nat'l Broad. Co., 232 Cal. Rptr. 668 (Ct. App. 1986).
178. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977).

"[m]atters concerning a person's medical treatment or condition are also generally considered private."[179] Just as the taking of photographs can constitute an intrusion,[180] so the publicity tort may apply to their distribution. For example, one court opined, "[w]e fail to see how autopsy photographs of the Plaintiffs' deceased relatives do not constitute intimate details of the Plaintiffs' lives or are not facts Plaintiffs do not wish exposed 'before the public gaze.'"[181] On the other hand, "there is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye."[182]

The core component of the publicity tort is, not surprisingly, that the defendant gave publicity to this private information. The relevant RESTATEMENT (SECOND) OF TORTS comment provides:

> it is not an invasion of the right of privacy, within the rule stated in this Section, to communicate a fact concerning the plaintiff's private life to a single person or even to a small group of persons. On the other hand, any publication in a newspaper or a magazine, even of small circulation, or in a handbill distributed to a large number of persons, or any broadcast over the radio, or statement made in an address to a large audience, is sufficient to give publicity within the meaning of the term as it is used in this Section. The distinction, in other words, is one between private and public communication.[183]

In this context, *Vassiliades v. Garfinckel's, Brooks Brothers* is instructive.[184] A patient brought an action against her plastic surgeon for invasion of privacy (publicity) after the surgeon used "before" and "after" photographs of her (taken with her consent) in promotional events at a department store and on television.[185] Evidence had been offered at trial by the plaintiff that "after agonizing over losing her youthful appearance and contemplating plastic surgery for many years, she underwent plastic surgery and kept her surgery secret, telling only family and very intimate friends."[186] For the court, there was no touchstone regarding who had seen the photographs or even whether her name had been published. Rather "[t]he nature of the publicity ensured that it would reach the public."[187]

This contrasts with *Robert C. Ozer, P.C. v. Borquez*.[188] The plaintiff's partner was diagnosed with AIDS and the plaintiff himself was advised to take

---

179. Doe v. Mills, 536 N.W.2d 824, 829 (Mich. Ct. App. 1995) (citation omitted).

180. *See* Estate of Berthiaume v. Pratt, 365 A.2d 792, 793 (Me. 1976).

181. Reid v. Pierce County, 961 P.2d 333, 341 (Wash. 1998).

182. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b. (1977).

183. RESTATEMENT (SECOND) OF TORTS § 652D cmt. a. (1977).

184. *See* 492 A.2d 580, 585 (D.C. 1985).

185. *Id.* at 584.

186. *Id.* at 587.

187. *Id.* at 588.

188. 940 P.2d 371 (Colo. 1997).

an HIV test.[189] Asking for confidence the plaintiff, an associate at a law firm, told his law firm president that he was gay, that he needed to be tested, and wished for some help covering a previously scheduled deposition.[190] One-week later the plaintiff was terminated, but not before he discovered that the information had been shared with everyone in the law firm.[191] The court reversed a jury verdict in the plaintiff's favor on a "publicity" count because of a defective jury instruction; the trial court had required only that the private information be "published" to another.[192] As the Colorado Supreme Court concluded, "the public disclosure requirement renders [defendant] liable for [plaintiff's] invasion of privacy claim only if [defendant] disclosed [plaintiff's] situation to a large number of persons or the general public."[193] As discussed below, *Vassiliades* and *Ozer* are not at odds with each other. Rather, modern courts recognize a more granular interpretation of the publicity tort. The "publicity" can occur either: (1) through "private" channels, thus triggering an additional requirement of a considerable number of recipients; or (2) through a "public" channel, anything from a sign in a shop window to a television broadcast, in which case there is no additional numerical touchstone.[194]

Given that the action rotates around private facts being made public, plaintiffs will have weaker cases when there has been some level of self-disclosure. *Stratton v. Krywko*, the television documentary case discussed above, was close to the line.[195] The defendants had successfully argued in their motion for summary judgment that the information disclosed about the plaintiff (such as her face, x-ray/cat scan data, status, prognosis, and Prozac prescription) was already public.[196] The appellate court agreed with regard to many of the items (for example, a public street accident, the police report of the accident) although others (e.g., scans) were not specifically identified during the broadcasts as hers.[197] However, the court considered that there was an issue of triable fact whether her Prozac prescription was known to "everybody" as argued by defendants or known to only a "select number of close friends and family."[198] As the court recognized, "[p]laintiff's argument has merit. Disclosing a fact to a small number of confidants does not equate to making the information public."[199]

Another issue that arises in publicity cases is whether the publicity reaches the "highly offensive" threshold. This question of offensiveness to a reasonable person is an issue of fact for the jury. For example, the court in *Vassiliades*

---

189. *Id.* at 373.
190. *Id.* at 374.
191. *Id.*
192. *Id.* at 379.
193. *Id.*
194. *See* discussion accompanying *infra* note 324.
195. No. 248669, 2005 Mich. App. LEXIS 23 (Mich. Ct. App. Jan. 6, 2005).
196. *Id.* at *12.
197. *Id.* at *14.
198. *Id.* at *15.
199. *Id.*

would not substitute its own views for a jury determination that the publication of "before" and "after" photographs met this test.[200]

The publicity tort can be defeated in the case of the qualified "legitimate public interest in the publication," either at common law or when the First Amendment is implicated.[201] Notwithstanding, when balancing out these interests, courts tend to favor the individual's right to privacy:

> The line is to be drawn when the publicity ceases to be the giving of information to which the public is entitled, and becomes a morbid and sensational prying into private lives for its own sake, with which a reasonable member of the public, with decent standards, would say that he had no concern.[202]

Gilbert v. Medical Economics Co.[203] concerned an article in defendant's magazine that discussed incidents of alleged malpractice committed by the plaintiff anesthesiologist. The article discussed the plaintiff's history of psychiatric and related personal problems in making the argument that there had been a breakdown in the regulatory system.[204] The court affirmed the defendant's summary judgment on the application of the defense noting "the legitimate public interest of warning potential future patients, as well as surgeons and hospitals, of the risks they might encounter in being treated by or in employing the plaintiff."[205]

The most difficult issue in these public interest cases is the assessment of the value of the specific identification. Consider again *Stratton v. Krywko*, where the defendants persuaded the trial court that the First Amendment protected their "Night in the E.R." documentary as newsworthy or educational.[206] The court reaffirmed the duality of this inquiry: "not only must the overall subject-matter be newsworthy, but also the particular facts [regarding the plaintiff] revealed."[207] On these facts, the court considered summary adjudication to be improper.[208] When dealing with this issue the courts, as noted in *Vassiliades*,[209] seek a "logical

---

200. Vassiliades v. Garfinkel's, Brooks Bros., 492 A.2d 580, 588 (DC. 1985).

201. *Id.* at 588-89; *see also* Gilbert v. Med. Econ. Co., 665 F.2d 305, 308 (10th Cir. 1981); Robert C. Ozer, P.C. v. Borquez, 940 P.2d 371, 378 n.8 (Colo. 1997) (discussing First Amendment's applicability); Fisher v. Dep't of Health, 106 P.3d 836, 841 (Wash. Ct. App. 2005) (holding that "the government *may* have had *no* legitimate interest in the dissemination of this private information sufficient to outweigh Ms. Fisher's protected privacy interest. But she must show that the extent of the dissemination outweighed her own privacy interest").

202. RESTATEMENT (2ND) OF TORTS, § 652D cmt. h (1977).

203. 665 F.2d 305 (10th Cir. 1981).

204. *Id.* at 307-08.

205. *Id.* at 309.

206. Stratton v. Krywko, No. 248669, 2005 Mich. App. LEXIS 23, at *15-16 (Mich. Ct. App. Jan. 6, 2005).

207. *Id.* at *20.

208. *Id.*

209. Vassiliades v. Garfinkel's, Brooks Bros., 492 A.2d 580, 585 (D.C. 1985).

nexus" between the legitimate public interest and the particular publicity given to the plaintiff's private information.[210]

3. Confidentiality Actions.—As discussed above, the tort action for breach of confidence is disclosure-centric and dependent on context. There is also a chronology at play, and as persuasively argued by Leslie Francis, it is a chronology not a prioritization.[211] A patient exercises this right of privacy when he or she chooses to provide information to a physician; "[i]f it were otherwise, patients would be reluctant to freely disclose their symptoms and conditions to their physicians in order to receive proper treatment."[212] That information then ceases to be private vis-à-vis the physician. Thereafter, dissemination of that information by the physician is limited by the requirement of confidence.[213] "One of the fiduciary duties that a physician assumes when he or she undertakes to treat a patient is the duty to refrain from disclosing a patient's confidential health information unless the patient expressly or impliedly consents or unless the law requires or permits disclosure."[214]

The modern trend is to apply a tort-based breach of confidence action regarding unauthorized disclosure of medical information.[215] For example, in *Biddle v. Warren General Hospital*, the court recognized both healthcare provider liability for either "unprivileged disclosure to a third party of nonpublic medical information that a physician or hospital has learned within a physician-patient relationship"[216] or third party liability for "inducing the unauthorized, unprivileged disclosure of nonpublic medical information."[217]

In enforcing the duty of confidentiality regarding medical information courts are particularly protective of medical records.[218] For example, in *Hageman v. Southwest General Health Center*,[219] the Supreme Court of Ohio reaffirmed its holding in *Biddle* and held a lawyer liable for breach of confidence when she passed medical records lawfully obtained in a divorce case to a prosecutor in a related matter.[220]

---

210. *Id.* at 589-90 (citations omitted).

211. Leslie Pickering Francis, *Privacy and Confidentiality: The Importance of Context*, 91 MONIST 52, 52-67 (2008).

212. Overstreet v. TRW Commercial Steering Div., 256 S.W.3d 626, 642 (Tenn. 2008) (citations omitted).

213. TOM L. BEAUCHAMP & JAMES F. CHILDRESS, PRINCIPLES OF BIOMEDICAL ETHICS 410 (4th ed. 1994).

214. *Overstreet*, 256 S.W.3d at 642 (citations omitted).

215. *See* McCormick v. England, 494 S.E.2d 431, 437 (S.C. Ct. App. 1997).

216. 715 N.E.2d 518, 523 (Ohio 1999).

217. *Id.* at 528.

218. Hageman v. Sw. Gen. Health Ctr., 893 N.E.2d 153, 155-56 (Ohio 2008).

219. *Id.*

220. *Id.* at 157-58; *see, e.g.*, Burger v. Blair Med. Assocs., 964 A.2d 374 (Pa. 2009); Jeffrey H. v. Imai, Tadlock & Keeney, 101 Cal. Rptr. 2d 916, 918-19 (Ct. App. 2000), *overruled in part by* Jacob B. v. County of Shasta, 154 P.3d 1003, 1012 (Cal. 2007); Anonymous v. CVS Corp., 728 N.Y.S.2d 333, 335 (Sup. Ct. 2001) (discussing pharmacy records).

Although there is no public interest defense to breach of confidence,[221] "a physician or hospital is privileged to disclose otherwise confidential medical information in those special situations where disclosure is made in accordance with a statutory mandate or common-law duty, or where disclosure is necessary to protect or further a countervailing interest which outweighs the patient's interest in confidentiality."[222] As with the statutory and regulatory confidentiality codes discussed below, breach of confidentiality actions can be met by defensive arguments that the disclosure was compelled by law,[223] is in the best interest of the patient or others,[224] or the patient has given express or implied consent to the disclosure.[225]

E. Ethical Restraints

Just as system architecture creates a soft law alternative to boundary law or governmental coercion, so the existing ethical boundaries that hover over the physician-patient relationship create a soft law approach to modulating the behaviors of some social network actors.

Basic medical professional ethics structures map quite well to the common law confidentiality and privacy restraints. Thus, the American Medical Association (AMA) Code of Medical Ethics combines its disclosure-centric requirement of confidence ("The physician should not reveal confidential information without the express consent of the patient") with the principle's instrumental justification ("The patient should feel free to make a full disclosure of information to the physician in order that the physician may most effectively provide needed services").[226] Similarly, the AMA's approach to collection-centric rules includes an "intrusion"-like privacy principle demanding protection of patient privacy as it relates to physical [privacy] "which focuses on individuals and their personal spaces."[227] However, the ethical rules also extend to associational ("family or other intimate relations"), informational ("specific personal data"), and decisional privacy ("personal choices").[228]

As discussed above, the legal domain's case-by-case approach to physician-patient privacy has added few bright line rules to the basic seclusion-intrusion or related mandates. In contrast, the AMA principles do bright line some specific fact-patterns.

---

221. *See* Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580, 591 (D.C. 1985).

222. *Biddle*, 715 N.E.2d at 524.

223. McCormick v. England, 494 S.E.2d 431, 439 (S.C. Ct. App. 1997).

224. *Id.*

225. Snavely v. AMISUB of S.C., Inc., 665 S.E.2d 222, 225 (S.C. Ct. App. 2008), *cert. denied* (Apr. 10, 2009).

226. AMA, CODE OF MEDICAL ETHICS § 5.05—Confidentiality (2007), http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion505.shtml.

227. *Id.* § 5.059—Privacy in the Context of Health Care, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5059.shtml.

228. *Id.*

Thus, physicians who participate in "interactive online sites that offer email communication" are expected to adhere to the AMA's guidelines on email.[229] It might seem that these guidelines would apply only to the email-like features grafted on to social network sites. However, the AMA opinion could be interpreted to provide guidelines for broader physician participation online and so prohibit the establishment of a physician-patient relationship through an online social network. Further, if a physician-patient relationship already existed such guidelines would require informed consent as to the limitations and risks associated with social network communication, and demand a regard for privacy and confidentiality that may be unattainable in the online social network context.[230]

The AMA ethical guidelines specifically address both contemporaneous and recorded observation of physician-patient interactions, scenarios that may point to the correct approach to social network "broadcasts" such as Facebook posts or Twitter streams. For example, the ethical approach to "outside observers"[231] requires their prior agreement to confidentiality and their presence is conditioned on "the patient's explicit agreement."[232] Similarly, with regard to filming and broadcasting encounters, the "educational objective can be achieved ethically by filming only patients who can consent."[233] Such consent must be obtained for both the filming and subsequent broadcasting.[234] Any such consent must be informed and thus is predicated on: "[A]n explanation of the educational purpose of film, potential benefits and harms (such as breaches of privacy and confidentiality), as well as a clear statement that participation in filming is voluntary and that the decision will not affect the medical care the patient receives."[235] Furthermore, the guidelines assume that the filming and broadcast will be limited to healthcare professionals and their students. If any broader audience is contemplated, that must be the subject of an additional, explicit consent.[236]

The framing of both the provisions on outside observers and filming are

---

229. *Id.* § 5.027(3)—Use of Health-Related Online Sites, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5027.shtml.

230. *Id.* § 5.026—The Use of Electronic Mail (2008-09), http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5026.shtml.

231. *Id.* § 5.0591—Patient Privacy and Outside Observers to the Clinical Encounter, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion50591.shtml (defining "outside observers" as "individuals who are present during patient-physician encounters and are neither members of a health care team nor enrolled in an educational program for health professionals").

232. *Id.*

233. *Id.* § 5.045(1)-(2)—Filming Patients in Health Care Settings, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5045.shtml.

234. *Id.*

235. *Id.* § 5.046—Filming Patients for the Education of Health Professionals, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5046.shtml.

236. *Id.*

sufficiently analogous to Internet broadcasting through social network sites that the additional considerations regarding confidentiality and informed consent are significant. First, the AMA notes that, "[p]hysicians should avoid situations in which an outside observer's presence may negatively influence the medical interaction and compromise care."[237] Second, "physicians should be aware that filming may affect patient behavior during a clinical encounter. The patient should be given ample opportunity to discuss concerns about the film, before and after filming, and a decision to withdraw consent must be respected."[238] Third, the ethical rules that acknowledge the requirement for explicit consent are based on the recognition that "filming cannot benefit a patient medically and may cause harm."[239]

F. HIPAA and Related Regulatory Models

Although reasonably well-developed areas of law by the late 1990s, the breach of confidence tort and related state statutes[240] were deemed inadequate to meet the needs of electronic, interoperable billing, and records systems. Starting in 2000, therefore, the breach of confidence tort has been supplemented by HIPAA, a federal confidentiality code (albeit one that is mislabeled as dealing with "privacy").[241]

Today, the HIPAA code is the most important source of regulation regarding disclosures of patient information by healthcare providers.[242] It is not the exclusive source because HIPAA is quite limited in its reach[243] and only partially preempts state confidentiality laws.[244] Much of the HIPAA regulatory framework is not directed at protecting patient information but creating the "exceptional" processes by which such data may be disseminated (such as patient consent) or creating broad safe harbors for public health, judicial, and regulatory

---

237. *Id.* § 5.0591—Patient Privacy and Outside Observers to the Clinical Encounter, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion50591.shtml.

238. *Id.* § 5.046(1)-(2)—Filming Patients for the Education of Health Professionals, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5046.shtml.

239. *Id.* § 5.045(2)—Filming Patients in Health Care Settings, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5045.shtml.

240. *See, e.g.*, CAL. CIV. CODE §§ 56–56.37 (West 2007); MONT. CODE ANN. §§ 50-16-501 to -553 (West Supp. 2009); WASH. REV. CODE ANN. §§ 70.02.005 to -.904 (West 2002 & Supp. 2009); WIS. STAT. § 146.83 (West Supp. 2009).

241. 45 C.F.R. § 164.500-534 (2009).

242. HIPPA Basics: Medical Privacy in the Electronic Age, http://www.privacyrights.org/fs/fs8a-hipaa.htm.

243. *See generally* Nicolas P. Terry, *What's Wrong With Health Privacy?*, 5 J. HEALTH & BIO. L. 1-32 (2009).

244. 45 C.F.R. §§ 164.500-534 (2009).

institutions.[245] Additionally, there have been strong critiques of the Office of Civil Rights in its approach to enforcing the regulations.[246] Some of the complaints about HIPAA's limitations should be addressed as a result of the Health Information Technology for Economic and Clinical Health Act, (HITECH), Subtitle D,[247] (part of the American Recovery and Reinvestment Act of 2009[248]). For example, "Business Associates" are no longer indirectly regulated through terms in their contracts with "Covered Entities" but are directly subject to the HIPAA code,[249] including its penalties.[250] HITECH seeks to respond to criticisms about HIPAA's lack of an educative goal, requiring regulations on educating health providers[251] and an initiative to "enhance public transparency regarding the uses of protected health information."[252] The legislation requires new regulations to strengthen the proportionality ("minimum necessary" under HIPAA) of disclosures[253] and strengthened restrictions on the use of protected health information for marketing purposes.[254] Enforcement should improve because of both tighter definitions of breaches of the code[255] and additional enforcement through state attorneys general.[256] Although there is still no private right of action, there will be a system designed to distribute a percentage of civil penalties or settlements collected from providers to injured patients.[257]

Notwithstanding the HIPAA approach to preemption, the HIPAA "floor," continues.[258] Further, the exact changes to the confidentiality code will depend on regulations made pursuant to the enabling legislation included in HITECH.

Although the HIPAA code and this forthcoming "version 2.0" are relevant

---

245. *See, e.g., id.* §§ 164.508, 164.510, 164.512.

246. *See, e.g.*, Kirk J. Nahra, *The HIPAA Enforcement Era Begins!*, WILEY REIN LLP, Aug. 2008, *available at* http://www.wileyrein.com/publication_newsletters.cfm?id=10&publication_id=13717; Anne Zieger, *Why Toughen HIPAA When Nobody Enforces It?*, FIERCE HEALTHIT, Jan. 25, 2009, *available at* http://www.fiercehealthit.com/story/why-toughen-hipaa-when-nobody-enforces-it/2009-01-25.

247. Health Information Technology for Economic and Clinical Health Act, Pub. L. No. 111-5, §§ 13001-13424, 123 Stat. 226.

248. American Recovery and Reinvestment Act of 2009, Pub. L. No. 111-5, 123 Stat. 115 (codified as amended in scattered sections of 2 U.S.C., 5-8 U.S.C., 10 U.S.C., 12 U.S.C., 15-16 U.S.C., 18-20 U.S.C., 25-26 U.S.C., 29 U.S.C., 31 U.S.C., 32 U.S.C., 38 U.S.C., 40-42 U.S.C., 45-47 U.S.C., 49 U.S.C.).

249. *Id.* § 13401(a)-(b).

250. *Id.* § 13404(c).

251. *Id.* § 13403(a).

252. *Id.* § 13403(b).

253. *Id.* § 13405(b).

254. *Id.* § 13406(a).

255. *Id.* § 13409-10.

256. *Id.* § 13410(e).

257. *Id.* § 13410(c).

258. *Id.* § 13421.

to the regulation of the social network fact patterns discussed in this article, they are of less importance than in traditional, offline healthcare "boundary" scenarios. Running a Twitter feed from inside a hospital or physician blog posts that identify patients would seem to implicate HIPAA's "covered entity" requirements as far as confidentiality and consent. However, HIPAA still only applies to data entrusted to and subsequently disclosed by healthcare providers. Thus, patient health information that is posted to a social network site by someone other than a covered entity (e.g., by the patient) will not trigger HIPAA. Perhaps the most important limitation of HIPAA relevant to this Article is that the federal code does not create boundaries as to the collection of patient information (e.g., by insurers, employers or even physicians surfing patient profiles), but only its disclosure. As a result, most of the "boundary" analysis that follows will rotate around common law theories of liability.

III. SETTING BOUNDARIES FOR PHYSICIANS AND PATIENTS

Patients and their healthcare providers are robust users of global and enterprise wide networks. However, the two groups seldom intentionally interact using such tools,[259] notwithstanding governmental and healthcare institutions interest in promoting online interactions such as researching efficient healthcare interventions or sharing electronic medical records.[260] More than 61% of U.S. adults search for health information online.[261] Sustained growth in patient enthusiasm for online interactions notwithstanding,[262] many physicians still view direct contact with patients via email as time-consuming tasks best left to staff[263]

---

259. *See* Nicolas P. Terry, *Prescriptions sans Frontières (or How I Stopped Worrying About Viagra on the Web but Grew Concerned About the Future of Healthcare Delivery)*, 4 YALE J. HEALTH POL'Y L. & ETHICS 183, 186 (2004) [hereinafter Terry, *Prescriptions sans Frontières*] (describing impact Internet has on doctor-patient relationship). *But see* Jaymes Song, *In Hawaii, the Doctor Is Always in-Online*, NEWSVINE, Jan. 15, 2009, http://www.newsvine.com/_news/2009/01/15/2313309-in-hawaii-the-doctor-is-always-in-online (describing exceptions to the dearth of online physician-patient interactions).

260. *See, e.g.*, Nicolas P. Terry, *Personal Health Records: Directing More Costs and Risks to Consumers?*, 1 DREXEL L. REV. 216 (2009) (discussing growth of commercial personal health records models); Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681, 691-96 (discussing drivers behind move to electronic records); *see also* Nicolas P. Terry, *To HIPAA, A Son: Assessing The Technical, Conceptual, and Legal Frameworks for Patient Safety Information*, 12 WIDENER L. REV. 133 (2005).

261. Fox & Jones, *supra* note 63, at 2.

262. Paul Rosen & C. Kent Kwoh, *Patient-Physician E-mail: An Opportunity to Transform Pediatric Health Care Delivery*, 120 PEDIATRICS 701 (2007); Hardeep Singh et al., *Older Patients' Enthusiasm to Use Electronic Mail to Communicate With Their Physicians: Cross-Sectional Survey*, 11 J. MED. INTERNET RES. e.18 (2009), http://www.jmir.org/2009/2/e18.

263. Terry, *Prescriptions sans Frontières*, *supra* note 259, at 227.

or creating unacceptable time pressures during consultations.[264] The AMA remains concerned that email contact will damage the traditional framework of the physician-patient relationship.[265] Meanwhile regulators and prosecutors take the position that online practice encourages opportunistic online relationships designed to encourage the illegal distribution of prescription drugs.[266]

To this dystopian online world of physicians and patients now must be added category-blurring behavior by both cohorts: physicians intending to blog or tweet to other physicians but reaching a far broader audience; patients exposing medical or genetic signals in apparently private Facebook posts; physicians disclosing sufficient personal information on their profile pages to concern a patient or raise a red flag during a pre-employment background check; and physicians entering perhaps unintended relationships with a small number of the undifferentiated cohorts they meet online.

This section seeks to identify some of the "pinch points" that could lead to legal exposure for healthcare providers or an array of surprises for patients.

A. Physicians' Social Information Online

Search is omnipresent as both a personal and professional tool. We can Google our friends or colleagues and increasingly may view it as unprofessional to take a meeting with someone un-researched.

In fact, 35% of adults have used the Internet to search "for information about physicians or other health professionals."[267] A slightly smaller group (28%) searches for information about institutional providers.[268] There is a robust correlation between the adults that search for information online and those who use social network sites; some 39% of the former cohort use social network sites.[269] Emerging consumer-driven healthcare models suggest that patients should research their potential providers.

There are innumerable, searchable databases regarding regulatory proceedings or litigation with adverse results for physicians. These include The National Practitioner Data Bank,[270] the Federation Physician Data Center,[271] and

---

264. Henry W.W. Potts & Jeremy C. Wyatt, *Survey of Doctors' Experience of Patients Using the Internet*, 4 J. MED. INTERNET RES. e5 (2002), http://www.jmir.org/2002/1/e5. *See also* Pauline W. Chen, *Medicine in the Age of Twitter*, N.Y. TIMES, June 11, 2009, http://www.nytimes.com/2009/06/11/health/11chen.html?_r=2; The Efficient MD—Life Hacks for Healthcare, http://efficientmd.blogspot.com/2008/04/ten-trends-in-american-medicine.html (Apr. 24, 2008, 12:22) (noting that the tenth top trend in healthcare is that Information Technology Will Fall Short of Promises).

265. AMA, CODE OF MEDICAL ETHICS § 5.026—The Use of Electronic Mail, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5026.shtml.

266. *See* Terry, *Prescriptions sans Frontières*, *supra* note 259, at 199-202.

267. Fox & Jones, *supra* note 63, at 35.

268. *Id.* at 46.

269. *Id.* at 15.

270. Health Care Quality Improvement Act of 1986, Pub. L. No. 99-660, §§ 401-32, 100 Stat.

resources maintained by state medical boards.[272] But these databases are not always complete (although the reach of the NPDB may be expanding[273]) and seldom will document social behavior.

In 2008, Thompson and colleagues evaluated the Facebook profiles of University of Florida medical students and residents; 44.5% of medical students had a Facebook account, but only 37.5% of profiles were made private.[274] The study found that, "[u]se is more common among students, and most chose to keep their profiles open to the public."[275] The study found that many of these accounts included personal information "that is not usually disclosed in a doctor–patient relationship."[276] A random sub-sample of such studied sites disclosed; "content that could be interpreted negatively," such as excess alcohol consumption and foul language.[277]

As discussed below employers routinely search the social network sites of applicants and employees even though this practice is not without legal risk.[278] Such disincentives notwithstanding, in the wake of high-profile hiring scandals the case can be made that no hospital or system should make a professional appointment without first performing a detailed background check using all available search tools; including searches of social network sites. Recall, for example, the data available about some of the Florida medical students.[279] Further, a social network profile might contain postings, uploaded and tagged data, or membership in online groups that could signal anything from substance abuse to attitudes about race or gender.

In the healthcare domain this background-checking issue is of increasing importance because of the rise of so-called 'negligent credentialing' suits brought by a patient against a health care facility allegedly injured as a result of the acts or omissions of a facility-credentialed physician. In *Larson v. Wasemiller*,[280] the Minnesota Supreme Court noted:

> Given our previous recognition of a hospital's duty of care to protect its

---

3743. *See generally* http://www.npdb-hipdb.hrsa.gov/.

271. FSMB, http://www.fsmb.org/m_fpdc.html (last visited Jan. 15, 2010).

272. *See, e.g.*, Virginia Board of Medicine Practitioner Information, http://www.vahealthprovider.com/ (last visited Jan. 15, 2010).

273. HHS NPRM, National Practitioner Data Bank for Adverse Information on Physicians and Other Health Care Practitioners: Reporting on Adverse and Negative Actions, 71 Fed. Reg. 14139-49 (Mar. 21, 2006).

274. Lindsay A. Thompson et al., *The Intersection of Online Social Networking with Medical Professionalism*, 23 J. GEN. INTERN. MED. 954, 954 (2008).

275. *Id.* at 956.

276. *Id.*; *see also* Jeff Cain, *Online Social Networking Issues Within Academia and Pharmacy Education*, 72 AM. J. PHARM. EDUC. 10 (2008).

277. Thompson et al., *supra* note 274, at 955-56.

278. *See infra* note 292 and accompanying text.

279. *See supra* notes 274-77 and accompanying text.

280. 738 N.W.2d 300 (Minn. 2007).

> patients from harm by third persons and of the analogous tort of negligent hiring, and given the general acceptance in the common law of the tort of negligent selection of an independent contractor, as recognized by the Restatement of Torts, we conclude that the tort of negligent credentialing is inherent in and the natural extension of well-established common law rights.[281]

The *Larson* court's 2007 opinion identified twenty-seven states that have recognized some form of the cause of action,[282] notwithstanding the difficult causation issues such suits pose.[283]

Although *Larson* recognized an action by the patient against the credentialing hospital, an important, additional legal implication was discussed in *Kadlec Medical Center v. Lakeview Anesthesia Associates*.[284] A patient in the plaintiff's medical center emerged from routine tubal ligation surgery in a permanent vegetative state.[285] The medical center settled a claim based on its respondeat *superior* for the alleged negligence of a drug-addicted anesthesiologist.[286] The medical center and its malpractice carrier then filed suit against the medical group where the anesthesiologist had previously practiced and the hospital where he worked and whose employees had discovered his drug abuse.[287] The group had terminated the anesthesiologist for drug abuse but had not reported him to the state medical board or NPDB.[288] Sixty-eight days after that termination members of the anesthesiology group submitted referral letters to a locum service that praised and recommended the physician yet failed to mention his drug abuse or that he had been terminated with a letter that included the phrase "[y]our impaired condition . . . puts our patients at significant risk."[289] The plaintiff medical center's detailed credentialing request to the hospital where the anesthesiologist had previously been credentialed was replied to with a brief and neutral statement of the dates of his prior employment.[290] At trial, the jury found for the plaintiff medical center on claims of intentional and negligent misrepresentation, and awarded $8.24 million (the settlement and attorney's fees in the original case).[291]

---

281. *Id.* at 306.

282. *Id.* at 306-07; *see also* Harrison v. Binnion, 214 P.3d 631, 635 (Idaho 2009) (holding peer review immunity statute does not create immunity for negligent credentialing); Frigo v. Silver Cross Hosp. & Med. Ctr., 876 N.E.2d 697 (Ill. App. Ct. 2007).

283. *See, e.g.*, Davis v. St. Francis Hosp., No. 00C-06-045-JRJ, 2002 Del. Super. LEXIS 272, at *9-10 (Del. Super. Ct. Oct. 17, 2002).

284. 527 F.3d 412 (5th Cir.), *cert. denied*, 129 S. Ct. 631 (2008).

285. *Id.* at 417.

286. *Id.*

287. *Id.* at 417-18.

288. *Id.* at 416.

289. *Id.* at 415.

290. *Id.* at 416.

291. *Id.* at 418.

On appeal the Fifth Circuit reversed the verdict against the hospital on the basis that under Louisiana law these facts did not give rise to an affirmative duty to disclose;[292] a decision that may have been somewhat generous to the hospital and that may not be replicated in other jurisdictions. However, the court did affirm the judgment against the medical reference letter writers for affirmative misrepresentation, noting that "[t]hese letters are false on their face and materially misleading."[293]

Healthcare institutions making credentialing or hiring decisions currently face a dilemma when it comes to information about physicians contained in social network profiles. Although there may be some risks in searching against them (as discussed in the next section), the potential liability for making a personnel decision in the absence of such information likely tips the balance.

B. Patients' Health-Related Information Online

Health-related information posted online *by patients* might include open references to medical conditions or risk-taking (e.g., photographs of alcohol or drug abuse) or quite explicit signals of risky behaviors (e.g., membership of the Facebook page "I do really stupid stuff when I'm Drunk"[294]). Other signals may be more nuanced (e.g., membership of the Facebook fan page "A Glass of Wine Solves Everything"[295]). Equally, membership in some social groups related to health conditions, although a relatively small number of persons join such groups,[296] may operate as implicit signals regarding personal or family health (e.g., membership of Facebook group pages relating to Cancer Survivors,[297] Chronic Fatigue Syndrome,[298] or Autism Awareness[299]). Social network discussions by sufferers and survivors are frequently cited as an emergent area of powerful patient self-help.[300] But all such information may be of interest to

---

292. *Id.* at 422 ("The defendants did not have a fiduciary or contractual duty to disclose what it knew to [plaintiff]. And although the defendants might have had an ethical obligation to disclose their knowledge of [the anesthesiologist's] drug problems, they were also rightly concerned about a possible defamation claim if they communicated negative information about [him].").

293. *Id.* at 419.

294. I Do Really Stupid Stuff When I'm Drunk, http://www.facebook.com/group.php?gid=222270916 (last visited Feb. 12, 2010).

295. A Glass of Wine Solves Everything, http://www.facebook.com/home.php#/group.php?gid=2390228727 (last visited Jan. 15, 2010).

296. Fox, & Jones, *supra* note 63, at 17 (Only 6% of the cohort that looks for health information online "have started or joined a health-related group on a social networking site.").

297. Cancer Survivors, http://www.facebook.com/home.php#/group.php?gid=2214852731 (last visited Jan. 15, 2010).

298. Chronic Fatigue Syndrome or Myalgic Encephalomyelitis, http://www.facebook.com/group.php?gid=65675018622 (last visited Jan. 15, 2010).

299. Autism Awareness, http://www.facebook.com/home.php#/group.php?gid=2207942310 (last visited Jan. 15, 2010).

300. *See, e.g.*, Zachary A. Goldfarb, *Seeking a Cure, Patients Find a Dose of Conversation*

employers or health insurers, and hopefully with more beneficence, physicians who search against their profiles.

1. Employers and Insurers.—Published surveys in the general employment world suggest that somewhere from one-quarter[301] to one-half of employers search the social network sites of potential employees.[302] Surveyed employers took particular note of suggestions of alcohol or drug use, inappropriate photos or other posted information, and "unprofessional" screen names.[303] Of course, sometimes, employee misconduct hardly needs any searching. The viral nature of data posted on social network sites is immense. But a video made by two pizza chain employees violating various health codes attracted one million views on YouTube and resulted in felony charges for the employees.[304]

Employer scrutiny of social network profiles implicates some legal risk when information discovered therein migrates into employment decisions.[305] For example, under federal law there is the potential for a discrimination action if a candidate was not hired because of religious belief or a disability revealed or suggested on a social network site.[306] Some state laws prohibit a broader list of discriminations (e.g., sexual orientation in California[307]). Going further, some state laws apply privacy and non-discrimination principles to private activities by employees.[308]

Online, WASH. POST, July 21, 2008, at D01.

301. Heather Havenstein, *One in Five Employers Uses Social Networks in Hiring Process*, COMPUTERWORLD, Sept. 12, 2008, http://www.computerworld.com/s/article/9114560/one_in_five_employers_uses_social_networks_in_hiring_process (22%); *see also* Wei Du, *Job Candidates Getting Tripped Up by Facebook*, Aug. 14, 2007, http://www.msnbc.msn.com/id/20202935/; Melissa Newton, *Employers Use MySpace, Facebook to Screen Applicants*, NBC DFW, Nov. 19, 2008, http://www.nbcdfw.com/news/business/Employers-Use-MySpace-Facebook-to-Screen-Applicants.html.

302. Adam Lisberg, *Employers May Be Searching Applicants' Facebook Profiles, Experts Warn*, DAILY NEWS (New York City), Mar. 10, 2008, http://www.nydailynews.com/money/2008/03/10/2008-03-10_employers_may_be_searching_applicants_fa.html (noting that 44% of employers searched profiles of job candidates on social networking sites; 39% searched a current employee's Facebook or MySpace pages).

303. Havenstein, *supra* note 301.

304. Stephanie Clifford, *Video Prank at Domino's Taints Brand*, N.Y. TIMES, Apr. 15, 2009, http://www.nytimes.com/2009/04/16/business/media/16dominos.html.

305. *See generally* Tari D. Williams & Abigail Lounsbury Morrow, *Want to Know Your Employees Better? Log on to a Social Network: But, Be Warned, You May Not Like What You See*, 69 ALA. LAW. 131, 132 (2008) (describing an employer's exposure to liability through use of social networking sites).

306. Civil Rights Act of 1964, 42 U.S.C. § 2000e-2 (2006); Americans with Disabilities Act of 1990, 42 U.S.C. 12101 (2006).

307. CAL. GOV'T CODE § 12940(a) (West 2005 & Supp. 2006).

308. *See, e.g.*, CAL. LAB. CODE § 96(k) (West Supp. 2010); COLO. REV. STAT. ANN. § 24-34-402.5(1) (West 2008) ("It shall be a discriminatory or unfair employment practice for an employer to terminate the employment of any employee due to that employee's engaging in any lawful

Information posted in the pseudo-secluded world of a social network site could signal certain genetic information.[309] This issue is clearly on the radar of the Equal Employment Opportunity Commission (EEOC) as evidenced by a recent Notice of Proposed Rulemaking (NPRM) issued under the Genetic Information Nondiscrimination Act of 2008 (GINA).[310]

GINA, signed into law in May 2008, broadly prohibits discrimination by employers and health insurers based upon genetic information. One of GINA's key provisions is to characterize an "employer,"[311] "employment agency,"[312] "labor organization,"[313] or "labor-management committee controlling apprenticeship or other training or retraining"[314] that "request[s], require[s], or purchase[s] genetic information with respect to an employee or a family member of the employee" as having engaged in an "unlawful employment practice."[315] GINA offers several safe harbors including "where an employer purchases documents that are commercially and publicly available (including newspapers, magazines, periodicals, and books, but not including medical databases or court records) that include family medical history."[316] In the EEOC's 2009 NPRM under GINA this exception is expanded to include "electronic media, such as information communicated through television, movies, or the Internet, except that a covered entity may not research medical databases or court records, even where such databases may be publicly and commercially available, for the purpose of obtaining genetic information about an individual."[317] In its commentary, EEOC invited "public comment on whether there are sources similar in kind to those identified in the statute that may contain family medical history and should be included either in the group of excepted sources or the group of prohibited sources, such as personal Web sites, or social networking sites."[318] An EEOC decision to take the latter approach and to wall-off genetically-related social network data from employer or insurer use would signal the first use of an inalienability rule in the social network regulatory space.

---

activity off the premises of the employer during nonworking hours . . . .").

309. For example, membership on a certain Facebook page might signal about family concerns regarding Type I diabetes (juvenile diabetes). *See* Find a Cure for Juvenile Diabetes, facebook.com/group.php?gid=2204811909 (last visited Feb. 12, 2010).

310. Notice of Proposed Rule-Making, Regulations Under the Genetic Information Nondiscrimination Act of 2008, 74 Fed. Reg. 9056-01 (Mar. 2, 2009) (to be codified at 29 C.F.R. pt. 1635); Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-233, 122 Stat. 881.

311. *Id.* § 202(b).

312. *Id.* § 203(b).

313. *Id.* § 204(b).

314. *Id.* § 205(a).

315. *Id.* §§ 205(a), 205(b).

316. *Id.* §§ 202(b)(4), 203(b)(4), 204(b)(4), 205(b)(4).

317. Notice of Proposed Rule-Making, Regulations Under the Genetic Information Nondiscrimination Act of 2008, 74 Fed. Reg. 9056-01 (Mar. 2, 2009) (to be codified at 29 C.F.R. pt. 1635).

318. *Id.* at 9063.

In the meantime employers and insurers likely will argue that the law of boundaries has little relevance to their activities. First, the intrusion tort would not apply to a non-corporeal (or informational) seclusion. Second, any publicity action should fail because the information searched is not "private" as it has been disclosed to the social network user's "friends," although the use of the discovered information does not satisfy the "publicity" requirement; the broadcast "public" channel property is inapplicable and because the information is only used "internally," plaintiff cannot meet the numerical touchstone required for "private" channel cases.

The decisional law suggests some validity regarding the second of these publicity arguments, at least in most cases of minimal distribution. Notwithstanding and as argued below, the information should be viewed as "private" when the user has applied privacy and security settings.

However, employers and insurers should be less sanguine about the inapplicability of the seclusion tort. Case law already recognizes areas of seclusion in otherwise public areas;[319] the question that is open is whether an application of security and privacy settings will be the touchstone for delineating a secluded space. The non-corporeal argument is more difficult. To an extent the courts will face a core entitlement question; whether to consign to history the trespass-like roots of the intrusion tort and apply it more liberally to informational privacy. If they take this latter, less existential, approach the appropriate doctrinal solution will be to pivot the tort around the offensiveness of the intrusion rather than the locus of the seclusion.[320]

2. Physician Use of Posted Social Information.—Employers and health insurers may have understandable business reasons for searching online profiles. But should physicians research their patients? And what should be done with such information diagnostically?

Of course, not all patient-posted information allows for identification of specific patients. As such, aggregated discussions by de-identified patients provides an educational opportunity for physicians who wish to learn more about generalized care models and patient perceptions and experiences associated with particular illnesses or diseases.[321]

However, Moreno and colleagues examined the profile pages of self-described sixteen- and seventeen-year-olds in the "class of 2008" MySpace group, and found that most were identifiable by name, photograph, location and that "[n]early half of the adolescents . . . publicly disclosed sexual activity, alcohol use, tobacco use, or drug use."[322] A similar study of sixteen- to eighteen-year-olds across several social network sites by Williams and colleagues found

---

319. *See supra* note 105 and accompanying text.

320. *See supra* note 103 and accompanying text.

321. Salil A. Mehta, *What Can Physicians Learn from the Blogs of Patients with Uveitis?*, 15 OCULAR IMMUNOLOGY AT INFLAMMATION 421, 423 (2007).

322. Megan A. Moreno et al., *What Are Adolescents Showing the World About Their Health Risk Behaviors on MySpace?*, MEDSCAPE GEN. MED. (2007), *available at* http://medscape.com/viewarticle/563320.

"84% of profiles and blog discussions containing some type of risk-taking behaviors," with nearly 50% of the participants at some risk of specific identification.[323]

The availability of this type of patient-specific information creates a classic emerging technology problem for physicians. May they ethically and legally access such information and, if they do, will they create a standard of care requiring scrutiny of such online data? The first question is easier to answer; general ethical standards suggest that physicians ask their patients' permission to access such information, even if it is publicly available. This stance dovetails with good risk management in that obtaining not just consent but informed consent regarding the access and use of such data will reduce the likelihood of either intrusion or malpractice actions. The second question, going to the standard of care, is more difficult to answer. At the very least professional specialty organizations (e.g., the American Psychiatric Association) should consider developing clinical practice guidelines on the subject with a view to preempting the indeterminacy of case-by-case development of the standard of care.

3. Third Parties Posting Patient Information.—Physicians will seldom be the direct source for patient-related health information that finds its way onto a social network site. Patients themselves, or their "friends" will have posted most such data. Some information may be sourced from providers (itself potentially implicating breach of confidence or HIPAA) but posted by meddlesome third parties.[324] Here, publicity and breach of confidence actions still may be applicable. The controversies in the recent Minnesota case of *Yath v. Fairview Clinics*,[325] began with a patient visit to a hospital clinic for STD testing. An acquaintance related to the patient's husband worked at the clinic as a medical assistant.[326] She recognized the patient and subsequently accessed her electronic medical record.[327] There she discovered that the patient tested positive for a STD and the fact that the patient had a new sexual partner.[328] The medical assistant passed on the information to another employee and the information eventually

---

323. Amanda L. Williams & Michael J. Merten, *A Review of Online Social Networking Profiles by Adolescents: Implications for Future Research and Intervention*, 43 ADOLESCENCE 253, 264 (2008).

324. *See, e.g.*, Meade v. Orthopedic Assocs. of Windham County, No. CV064005043, 2007 Conn. LEXIS 3424, at *7 (Conn. Super. Dec. 27, 2007), 2007 Conn. Super. LEXIS 3424 (holding when employee acquired and distributed patient records but action was only filed against health facility that "[a] cause of action for invasion of privacy will not lie where the defendant did not directly publicize the private facts about the plaintiff even though 'publicity was a natural and foreseeable consequence' of the defendant's actions"). Of course the institution may be responsible vicariously in some circumstances and might still face HIPAA liability.

325. 767 N.W.2d 34, 58 (Minn. Ct. App. 2009).

326. *Id.* at 38.

327. *Id.*

328. *Id.*

became known to the patient's estranged husband.[329] After an investigation the medical assistant was terminated by the hospital.[330] Shortly thereafter a MySpace page was created containing information from the patient's medical record.[331] The page was online for approximately twenty-four hours and likely was viewed by only six people.[332] The patient brought action against most of the actors and the hospital on several theories including public disclosure of private facts and the private right of action provided by Minnesota's Health Records Act.[333] The trial court granted the defendants' motions for summary judgment.[334]

On appeal the court remanded the issue of the statutory private right of action asserted by the patient against the hospital and the medical assistant to the trial court, but not before ruling that such a state private right of action was not preempted by the federal HIPAA code.[335] Instead, ruling that the provisions were complementary: "[r]ather than creating an 'obstacle' to HIPAA, Minnesota statutes section 144.335 supports at least one of HIPAA's goals by establishing another disincentive to wrongfully disclose a patient's health care record."[336] A similar analysis should apply to a common law action for breach of confidence by a healthcare provider.

The *Yath* court affirmed the summary judgment on the public disclosure count on the basis that the likely authors of the MySpace page had been dismissed from the action.[337] Notwithstanding, the court exhaustively examined the defendant's other contention that the "publicity" requirement[338] was not satisfied by posting to a social network site that was only available for a short time and viewed by a small number of people.[339] The court referenced a controlling Minnesota analysis of RESTATEMENT (SECOND) OF TORTS section 652D[340] establishing the "publicity" element was satisfied by proving either, "a single communication to the public," *or* "communication to individuals in such a large number that the information is deemed to have been communicated to the public."[341] The court viewed posting to a social network site as an example of the former type of public communication because "[t]his Internet communication is materially similar in nature to a newspaper publication or a radio broadcast

---

329. *Id.*

330. *Id.* at 39.

331. *Id.*

332. *Id.* at 39, 43.

333. *Id.* at 39. MINN. STAT. ANN. § 144.335 (West 2005) governed the case but has been replaced by MINN. STAT. ANN. § 144.298 (West Supp. 2010).

334. *Yath*, 767 N.W.2d at 40.

335. *Id.* at 50.

336. *Id.*

337. *Id.* at 45.

338. *See supra* text accompanying note 178.

339. *Yath*, 767 N.W.2d at 42-45.

340. *Id.* at 42.

341. *Id.*

because upon release it is available to the public at large."[342] Analogizing this brief web posting to "a late-night radio broadcast aired for a few seconds and potentially heard by a few hundred (or by no one)"[343] or "a poster displayed in a shop window,"[344] the court noted:

> It is true that mass communication is no longer limited to a tiny handful of commercial purveyors and that we live with much greater access to information than the era in which the tort of invasion of privacy developed. A town crier could reach dozens, a handbill hundreds, a newspaper or radio station tens of thousands, a television station millions, and now a publicly accessible webpage can present the story of someone's private life, in this case complete with a photograph and other identifying features, to more than one billion Internet surfers worldwide. This extraordinary advancement in communication argues for, not against, a holding that the MySpace posting constitutes publicity.[345]

The *Yath* court specifically noted that the MySpace profile in question was not one to which access had been restricted by "a password or some other restrictive safeguard."[346] Thus, it left hanging the same question as the one in *Moreno v. Hanford Sentinel, Inc.*,[347] where, as previously discussed, a college student's MySpace posting, critical of her hometown, found its way to the local newspaper.[348] If a social network site user applies security and privacy settings, would that render the site "secluded" for the purpose of initiating a breach of seclusion action or "private" for the purpose of resisting a publicity claim?

The most efficient approach for courts to adopt would be a bright line "posting" rule; that is, all posts, security or privacy settings notwithstanding, are public. Such an approach would avoid the inevitable and possibly interminable case-by-case debates whether "private" exposure of information to 10,100, or even 1000 friends would be akin to a public post.

However, that approach seems contrary to *Hill v. National Collegiate Athletic Ass'n*,[349] otherwise followed in *Moreno*. *Hill* upheld the NCAA's drug testing program in a suit brought by student athletes arguing violation of California's constitutional right to privacy.[350] Subsequently, it may be have been narrowed by the Supreme Court of California in *Sheehan v. San Francisco 49ers, Ltd.*,[351] a case dealing with security pat-downs at a football stadium. *Sheehan* re-

342. *Id.* at 43.
343. *Id.* at 44.
344. *Id.* at 45.
345. *Id.* at 44.
346. *Id.*
347. 91 Cal. Rptr. 3d 858 (Ct. App. 2009).
348. *See supra* text accompanying note 147.
349. 865 P.2d 633 (1994).
350. *Id.* at 669.
351. 201 P.3d 472 (Cal. 2009).

emphasized *Hill*'s statement about context: "assessment of the relative strength and importance of privacy norms and countervailing interests may differ in cases of private, as opposed to government, action."[352] *Sheehan* also stressed *Hill*'s observation that a plaintiff's privacy interests when bringing an action under California's constitutional privacy right "may weigh less in the balance"[353] if he or she "was able to choose freely among competing public or private entities in obtaining access to some opportunity, commodity, or service."[354]

Yet, in the context of the common law of boundaries, *Hill*'s words remain potent:

> Privacy rights also have psychological foundations emanating from personal needs to establish and maintain identity and self-esteem by controlling self-disclosure: "In a society in which multiple, often conflicting role performances are demanded of each individual, the original etymological meaning of the word 'person'—mask—has taken on new meaning. [People] fear exposure not only to those closest to them; much of the outrage underlying the asserted right to privacy is a reaction to exposure to persons known only through business or other secondary relationships. The claim is not so much one of total secrecy as it is of the right to *define* one's circle of intimacy—to choose who shall see beneath the quotidian mask. Loss of control over which 'face' one puts on may result in literal loss of self-identity, and is humiliating beneath the gaze of those whose curiosity treats a human being as an object."[355]

The key privacy expectation acknowledged by the law of boundaries is this "right to *define* one's circle of intimacy."[356] As citizens spend more of their time in online environments and make responsible use of privacy and security settings to disaggregate those with whom they interact, so the law should respect their defined circles of intimacy.

C. Physicians and Patients as "Friends"

Suppose a physician "friends" a patient or vice versa. Does such blurring of personal and professional relationships create concern in either the legal or ethical domains? In the case of the former the primary question will be whether such a blurred, technologically mediated relationship could give rise to the legally significant physician-patient relationship.[357] In the ethical domain, the

---

352. *Id.* at 479 (quoting *Hill*, 865 P.2d at 656).

353. *Id.* (quoting *Hill*, 865 P.2d at 657).

354. *Id.*

355. 865 P.2d at 647 (alteration in original) (citations omitted) (quoting Briscoe v. Reader's Digest Ass'n, Inc., 483 P.2d 34, 37 (Cal. 1971).

356. *See id.*

357. A related question is whether physician-patient contact through a social network could constitute the continuation of a relationship for the purposes of tolling a period of limitation. *See,*

question will come down to motive: is there a sense that the relationship is driven by the needs of the physician rather than the interests of the patient?

Again, context is important in unpacking the boundary issues. The appropriate question must be whether social or professional interests motivate the physician who follows a patient on Facebook or Twitter. If the motivation is social, then difficult boundary issues may arise. If professional (e.g., using social media to extend the treatment space), difficult risk management questions arise.

1. Creating a Physician-Patient Relationship.—Most of the scenarios discussed in this article assume the existence of a physician-patient relationship and then discuss how physician or patient online activities will play out against the healthcare regulatory matrix. Discussed, therefore, are scenarios such as physicians searching their patients' social network sites or micro-blogging about their treatment. Suppose, however, that there is no formed professional relationship at the point when a patient and a physician interact online. Could such interaction trigger the creation of a physician-patient relationship?

Such a relationship is both a conclusion and a term of art relied upon by the ethical and legal domains. As an ethical construct, it is the foundation of duties (and correlate expectations) of competence, respect, and confidence.[358] In the legal domain, the existence of a physician-patient relationship establishes the contractual responsibilities of the parties (such as the provision of services and the obligation to pay) and is the predicate for the finding of a legal duty; a requirement for tort recovery in the case of negligently provided care.[359]

These domain-specific questions engender the question: what does it take to create the physician-patient relationship? The doctrinal answer is that "the relationship is created when professional services are rendered and accepted for purposes of medical treatment."[360] The existence of a physician-patient relationship is usually a question of fact left to the jury.[361] In practice, therefore, the key issue is where the courts draw the summary judgment line.

---

e.g., Weaver *ex rel.* Weaver v. Univ. of Mich. Bd. of Regents, 506 N.W.2d 264, 266 (Mich. Ct. App. 1993); Griffith v. Brant, 442 N.W.2d 652, 654 (Mich. Ct. App. 1989). *See generally* Jewson v. Mayo Clinic, 691 F.2d 405, 408-09 (8th Cir. 1982) (discussing what constitutes evidence of a continuing physician-patient relationship for the purposes of determining the statute of limitations period for medical malpractice actions).

358. *See, e.g.*, AMA, *Principles of Medical Ethics* (2001), http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/principles-medical-ethics.shtml.

359. *See, e.g.*, Sterling v. Johns Hopkins Hosp., 802 A.2d 440, 445 (Md. 2002); Kruger *ex rel.* Estate of Kruger v. Jennings, No. 227480, 2002 WL 344268, at *3 (Mich. Ct. App. Apr. 12, 2002), *superseded by* 2002 WL 652098; Pittman v. Upjohn Co., 890 S.W.2d 425, 431 (Tenn. 1994).

360. Miller v. Sullivan, 214 A.2d 822, 823 (N.Y. App. Div. 1995).

361. *See, e.g.*, Irvin *ex rel.* Irvin v. Smith, 31 P.3d 934, 940-41 (Kan. 2001); Lyons v. Grether, 239 S.E.2d 103, 105 (Va. 1977); Walker v. Jack Eckerd Corp., 434 S.E.2d 63, 69 (Ga. Ct. App. 1993); Cogswell *ex rel.* Cogswell v. Chapman, 249 A.D.2d 865, 866 (N.Y. App. Div. 1998); Bienz v. Cent. Suffolk Hosp., 163 A.D.2d 269, 270 (N.Y. App. Div. 1990) ("Whether the physician's giving of advice furnishes a sufficient basis upon which to conclude that an implied physician-patient relationship had arisen is ordinarily a question of fact for the jury.").

Because of the consensual nature of the physician-patient relationship, courts must determine in these cases whether the physician consented to treat the patient.[362] Such consent can be express, implied,[363] or derived from a duty owed by the physician to another.[364] In short, "whatever circumstances evince the physician's consent to act for the patient's medical benefit."[365] This approach explains most of the decisions related to the clusters of fact-patterns that are relatively mature. For example, how courts navigate the distinction between the informal (or "curbside") consult[366] and the formal (or "bedside") consult,[367] deal with the responsibilities of on-call but non-treating physicians,[368] and respond to cases where patients are examined by physicians employed by others such as employers or insurers.[369]

---

362. "The physician may consent to the relationship by explicitly contracting with the patient, treating hospital, or treating physician. Or the physician may take certain actions that indicate knowing consent, such as examining, diagnosing, treating, or prescribing treatment for the patient." Lownsbury v. VanBuren, 762 N.E.2d 354, 362 (Ohio 2002).

363. *See, e.g.*, St. John v. Pope, 901 S.W.2d 420, 423 (Tex. 1995) (stating that a doctor-patient relationship can only be formed with the express or implied consent of physician).

364. *See* Bovara v. St. Francis Hosp., 700 N.E.2d 143, 146 (Ill. App. Ct. 1998) ("A consensual relationship can be found to exist . . . where a physician accepts a referral of a patient [from another physician]." (citations omitted)).

365. *Lownsbury*, 762 N.E.2d at 360.

366. *See, e.g.*, *Irvin*, 31 P.3d at 943 (holding that an "extension of the physician-patient relationship to include . . . [curbside] consultation would be contrary to public policy"); Oja v. Kin, 581 N.W.2d 739, 743 (Mich. Ct. App. 1998) (holding that "merely listening to another physician's description of a patient's problem and offering a professional opinion regarding the proper course of treatment is not enough [to form a patient-physician relationship]"); Corbet v. McKinney, 980 S.W.2d 166, 169 (Mo. Ct. App. 1998) (citing factors where a consulting physician may develop a patient-physician relationship with a patient whom the consulting physician has never met or spoken with). *Cf.* Gilinsky v. Indelicato, 894 F. Supp. 86 (E.D.N.Y. 1995) (determining if a patient-physician relationship exists between a patient and a consulting physician depends on whether the treating physician used independent judgment when accepting or rejecting advice of consulting physician); *Cogswell*, 249 A.D.2d at 866 (holding that a telephone call can create a patient-physician relationship if physician "affirmatively advises a prospective patient as to a course of treatment and it is foreseeable that the patient would rely on the advice" (quotations omitted)).

367. *See, e.g.*, Kelley v. Middle Tenn. Emergency Physicians, P.C., 133 S.W.3d 587, 595 (Tenn. 2004) (distinguishing on call physicians from those participating in informal physician to physician consults).

368. *See, e.g.*, Prosise v. Foster, 544 S.E.2d 331, 334 (Va. 2001) (holding that there was no patient-physician relationship because there was no evidence that physician agreed to take patient's case by agreeing to act as an on-call attending physician in a teaching hospital); Wazevich v. Tasse, No. 88938, 2007 Ohio App. LEXIS 4484, at *17 (Ohio Ct. App. Sept. 27, 2007) (finding that an on-call doctor and emergency room patient may develop a patient-physician relationship depending on the hospital's procedures and whether physician took affirmative action on behalf of the patient).

369. *See, e.g.*, Greenberg v. Perkins, 845 P.2d 530, 538 (Colo. 1993) (holding that an independent medical examiner had a duty of care to not cause examinee harm); Dyer v. Trachtman,

The cases dealing with technologically mediated, but not physical contact between physician and patient, are less transparent. It does seem clear that "a telephone call merely to schedule an appointment with a provider of medical services does not by itself establish a physician-patient relationship where the caller has no ongoing physician-patient relationship with the provider and does not seek or obtain medical advice during the conversation."[370] Similarly, merely scheduling a diagnostic test is likely insufficient.[371] As soon as there is engagement in the treatment process by the physician; however, the relationship may be held to exist.[372]

The case that is closest to a social network scenario is *Miller v. Sullivan*,[373] where a dentist telephoned a friend who was a physician between 9:30 a.m. to 10:00 a.m., and informed him that he believed he was having a heart attack.[374] The physician allegedly told the dentist "to come over and see him right away."[375] The dentist continued to see his own patients through the morning, however, and did not reach the physician's office until the early afternoon at which point he suffered a cardiac arrest.[376] The court upheld the defendant physician's summary judgment[377] by finding the physician owed the decedent no duty of care and therefore there was no breach of duty:

> Assuming that a physician renders professional service for purposes of medical treatment to a prospective patient who calls on the telephone when the physician tells the caller to come to his office right away, the record in this case conclusively establishes that decedent did not accept

---

679 N.W.2d 311, 314 (Mich. 2004) (holding that "an [independent medical examination] physician has a limited physician-patient relationship with the examinee . . . [with] limited duties to exercise professional care"); Harris v. Kreutzer, 624 S.E.2d 24, 32 (Va. 2006) (holding that "physician's duty is limited solely to the exercise of due care . . . as not to cause harm to the patient in actual conduct of the examination"); Heller v. Peekskill Cmty. Hosp., 198 A.D.2d 265, 265-66 (N.Y. App. Div. 1993) (citing factors plaintiff must prove to establish that an examining doctor consented to a patient-physician relationship).

370. Weaver *ex rel.* Weaver v. Univ. of Mich. Bd. of Regents, 506 N.W.2d 264, 266 (Mich. App. Ct. 1993).

371. Jackson v. Isaac, 76 S.W.3d 177, 184 (Tex. App. 2002).

372. Bienz v. Cent. Suffolk Hosp., 163 A.D.2d 269, 269, 270 (N.Y. App. Div. 1990) (holding that a telephone conversation that includes recommendation for a course of treatment may give rise to physician-patient relationship); Lam v. Global Med. Sys., Inc., 111 P.3d 1258, 1261 (Wash. Ct. App. 2005) (holding that ship-to-shore radio communication was sufficient to create physician-patient relationship under the facts of the case); *see also* Cogswell *ex rel.* Cogswell v. Chapman, 249 A.D.2d 865, 866-67 (N.Y. App. Div. 1998) (holding that telephone consult may establish a physician-patient relationship depending on physician's level of participation in patient's care).

373. 214 A.D.2d 822 (N.Y. App. Div. 1995).

374. *Id.* at 822.

375. *Id.* at 823.

376. *Id.*

377. *Id.*

> the professional service. Instead, decedent chose to pursue an entirely different course of conduct than that recommended by defendant.[378]

In conflating the issues of duty and breach, the *Miller* court made it less than clear whether a physician-patient relationship existed on these facts. Arguably, the court held that there was no such relationship because (and this is a different approach from the cases discussed above) the *patient* failed to agree to the relationship by rejecting the physician's advice.[379]

Physicians seem to understand the perils of creating an unexpected, offline physician-patient relationship. They show caution in social interactions (e.g., at social gatherings, parties, etc.). This caution will need to be extended to online interactions.

In the absence of a pre-existing physician-patient relationship the blog scenario gives rise to issues that are similar to those encountered by physicians in navigating email questions about health; more specifically, responding to unsolicited email.[380] When a non-patient poses a health-related question to a physician, be it through an email, a blog, or a social network site, the physician has two core options; to ignore the question or to answer it. Ignoring such a communication is not without some risks, particularly if the putative patient describes an emergency situation.[381] Any kind of personalized response, let alone any type of diagnosis or treatment advice, however, would likely create a jury issue over the creation of a physician-patient relationship, even if disclaimers accompanied the communication.[382] Rather, the only legally sound approach is for the physician to respond to an electronic inquiry with a standard form response, that in no way refers to the specific sender or the sender's disclosed information, which (1) informs the questioner that the physician does not answer such online questions, (2) supplies the questioner with the physician's offline office information in case the questioner would like to make an appointment, and (3) provides contact information for the emergency services and suggest the questioner contacts same if he or she cannot wait for an appointment during regular business hours.

2. Risk-Managing a Blurred Relationship.—The correlate of this scenario

---

378. *Id.*

379. *Id.*

380. *See generally* Gunther Eysenbach & Thomas L. Diepgen, *Responses to Unsolicited Patient E-mail Requests for Medical Advice on the World Wide Web*, 280 JAMA 1333, 1333 (1998).

381. *Cf.* Patricia C. Kuszler, *A Question of Duty: Common Law Legal Issues Resulting from Physician Response to Unsolicited Patient Email Inquiries*, J. MED. INTERNET RES. (2000), *available at* http://www.jmir.org.2000/3/e17; Mary V. Seeman & Bob Seeman, *E-psychiatry: The Patient-Psychiatrist Relationship in the Electronic Age*, 161 CAN. MED. ASS'N J. 1147 (1999), *available at* 1999 WLNR 189189 ("Clearly, the most judicious course of action is not to respond to email queries.").

382. *Cf.* Eric E. Shore, *Giving Advice on Social Networking Sites*, 85 MED. ECON. 18 (2008), *available at* 2008 WLNR 25457729.

also requires attention. If one assumes an existing physician-patient relationship and that the physician is utilizing social network tools to extend the treatment space, what are the liability risks? Regarding the use of email communication between patient and physician, the AMA stresses notification by the physician to the patient of the risks and limitations of such communication. These include, "potential breaches of privacy and confidentiality, difficulties in validating the identity of the parties, and delays in responses."[383] Any such communication should be preceded by informed consent regarding these risks.[384] Absent such setting of professional and technological expectations (and boundaries) liability risks may arise if a physician is not checking social network posts regularly (or regularly as the patient posts) and fails to see, say, a time-sensitive diagnostic signal.[385]

3. Appropriateness of "Friend" Relationships.—Suppose that there is an extant physician-patient and, hence professional relationship, but that a social or personal relationship subsequently develops through a social network intermediary. This phenomenon has received the most commentary regarding employment relationships in situations where employers seek to friend employees and exploit access to posted data such as opinions or photographs.[386]

At the extreme, social relationships between physicians and patients can involve sexual relationships.[387] The AMA characterizes "[s]exual contact that occurs concurrent with the patient-physician relationship" as "sexual misconduct."[388] Non-concurrent relationships may also be unethical "if the physician uses or exploits trust, knowledge, emotions, or influence derived from the previous professional relationship."[389] These concepts of trust, exploitation, and the primacy of patient well-being help to tease out the application of ethical principles to "friending" online.

Nadelson and Notman have helpfully explored these greyer areas of physician-patient relationships. They differentiate between "minor boundary *crossings*" that they do not regard as "exploitative" from those that they

---

383. AMA, CODE OF MEDICAL ETHICS § 5.026(3)—The Use of Electronic Mail (2003), http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion5026.shtml.

384. *Id.* § 5.026(4).

385. *See generally* Chen, *supra* note 264.

386. *See, e.g.*, Michelle Wilding, *Is Your Boss Your Friend or Foe?*, SYDNEY MORNING HERALD, May 19, 2009, http://www.smh.com.au/news/technology/biztech/is-your-boss-your-friend-or-foe/2009/05/18/1242498695453.html?page=fullpage#contentSwap1.

387. *See generally* Paul S. Appelbaum et al., *Sexual Relationships Between Physicians and Patients*, 154 ARCH. INTERN. MED. 2561 (1994); Linda J. Demaine, *'Playing Doctor' with the Patient's Spouse: Alternative Conceptions of Health Professional Liability*, 14 VA. J. SOC. POL'Y & L. 308 (2007).

388. AMA, CODE OF MEDICAL ETHICS § 8.14—Sexual Misconduct in the Practice of Medicine (1992), http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion814.shtml.

389. *Id.*

categorize as "damaging boundary *violations*."[390] For the purposes of this Article, the vocabulary Nadelson and Notman use to frame the issues is on point here. In particular, they state:

> An essential element of the physician's role is the idea that what is best for the patient must be the physician's first priority. Physicians must set aside their own needs in the service of addressing their patient's needs. Relationships, such as business involvements, that coexist simultaneously with the doctor–patient relationship have the potential to undermine the physician's ability to focus primarily on the patients' well being, and can affect the physician's judgment.[391]

Some physicians argue that the use of social network tools to extend the physician-patient relationship allows the patient to see the "human side" of the physician.[392] However, as Nadelson and Notman observe, "at times self-disclosure may be excessive and create difficulties. The patient may react negatively and it may seem like a role reversal if the doctor begins to disclose personal problems to the patient," and can create a "boundary problem because it can use the patient to satisfy the doctor's own needs for comfort or sympathy."[393] Specific ethical guidelines consistent with this approach caution physicians regarding, for example, discussion of politics[394] or "derogatory language or actions."[395] In short, the physician must be protective of the patient's needs, and not his own.

D. Physicians "Tweeting" or Posting About Their Work

The modern Hippocratic Oath will include language such as "I will respect the hard-won scientific gains of those physicians in whose steps I walk, and

---

390. Carol Nadelson & Malkah T. Notman, *Boundaries in the Doctor–Patient Relationship*, 23 J. THEORETICAL MED. 191, 192 (2002).

391. *Id.* at 195; *see also* AM. PSYCH. ASS'N, THE PRINCIPLES OF MEDICAL ETHICS WITH ANNOTATIONS ESPECIALLY APPLICABLE TO PSYCHIATRY 13 (2009), http://www.psych.org/MainMenu/PsychiatricPractice/Ethics/ResourcesStandards.aspx (follow "The Principles of Medical Ethics with Annotations Especially Applicable to Psychiatry" hyperlink) ("A psychiatrist shall not gratify his or her own needs by exploiting the patient.").

392. *See* Stacey Butterfield, *Twitter: A Medical Help, Hindrance or Hype?*, ACP INTERNIST, Apr. 2009, http://www.acpinternist.org/archives/2009/04/ twitter.htm; Carleen Hawn, *Take Two Aspirin and Tweet Me in the Morning: How Twitter, Facebook, and Other Social Media Are Reshaping Health Care*, 28 HEALTH AFFAIRS 361 (2009). *See generally* Chen, *supra* note 264.

393. Nadelson & Notman, *supra* note 390, at 197.

394. AMA CODE OF MEDICAL ETHICS § 9.012—Physicians' Political Communications with Patients and Their Families (1999), http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion9012.shtml.

395. AMA CODE OF MEDICAL ETHICS § 9.123—Disrespect and Derogatory Conduct in the Patient-Physician Relationship, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion9123.shtml.

gladly share such knowledge as is mine with those who are to follow."[396] The AMA Code of Medical Ethics includes in its description of the physician's role, "a teacher who imparts knowledge of skills and techniques to colleagues."[397] Not surprisingly physicians embrace new technologies to fulfill their educational responsibilities. However, posting or "tweeting" about their work is not without its risks.

1. Blogging and Posting.—According to 2008 research, 12% of Internet users (9% of all U.S. adults) "blog," while 33% of Internet users (24% of all adults) read blogs.[398] Kovic and colleagues estimated that there are over one thousand active English-language medical blogs, and found that these medical bloggers are highly educated and that many had previously published scientific papers.[399] Yet, only a relatively small number of participants in the medical blogosphere identified themselves as healthcare professionals.[400] Seeman[401] identified the six most highly used health-related blogs as BadScience.net (written by a U.K. physician who critiques media coverage of science),[402] Medgadget.com (written by MDs and biomedical engineers),[403] the journalist-run Wall Street Journal Health Blog,[404] SharpBrains (concentrating on "brain fitness" and "the cognitive health" market),[405] KevinMD.com (written by a New Hampshire-based primary care physician; its associated Twitter site, @kevinmd, has more than 20,703 "followers"),[406] and Diabetes Mine (a patient information and support blog).[407]

Lagu and colleagues examined 271 blogs written by healthcare providers and

---

396. The Hippocractic Oath: Modern Version, http://www.pbs.org/wgbh/nova/doctors/oath_modern.html (last visited Jan. 15, 2010).

397. AMA CODE OF MEDICAL ETHICS § 9.08—New Medical Procedures, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion908.shtml (last visited Jan. 15, 2010).

398. Aaron Smith, *New Numbers for Blogging and Blog Readership*, PEW INTERNET & AM. LIFE PROJECT, July 22, 2008, http://www.pewinternet.org/Commentary/2008/July/New-numbers-for-blogging-and-blog-readership.aspx.

399. *Id.*

400. Ivor Kovic et al., *Examining the Medical Blogosphere: An Online Survey of Medical Bloggers*, 10 J. MED. INTERNET RES. e28 (2008), http://www.jmir.org/2008/3/e28/; *cf.* Deirdre Kennedy, *Doctor Blogs Raise Concerns About Patient Privacy* (Nat'l Pub. Radio broadcast Mar. 13, 2008), *available at* http://www.npr.org/templates/story/story.php?storyId=88163567 (noting 120,000 medical blogs).

401. Neil Seeman, *Inside the Health Blogosphere: Quality, Governance and the New Innovation Leaders*, 7 ELECTRONICHEALTHCARE 101 (2008).

402. Bad Science, http://badscience.net/ (last visited Jan. 15, 2010).

403. Medgadget, http://medgadget.com/ (last visited Jan. 15, 2010).

404. Health Blog, http://blogs.wsj.com/health/ (last visited Jan. 15, 2010).

405. SharpBrains, http://www.sharpbrains.com/blog/ (last visited Jan. 15, 2010).

406. Kevin MD.com Medical Weblog, http://www.kevinmd.com/blog/ (last visited Apr. 1, 2010).

407. Diabetes Mine, http://www.diabetesmine.com/ (last visited Jan. 15, 2010).

found that 42.1% described interactions with individual patients and 16.6% included information detailed enough that patients could identify the provider or themselves.[408] Eight blogs included imaging related to patients and three blogs even showed identifiable photographs.[409] Patients were portrayed negatively in 17.7% of blogs; negative comments about the healthcare system appeared in 31.7% of blogs.[410]

Certain types of blog posts, each with different levels of attendant risk, can be identified.[411] The first, which will pose few legal risks, may be thought of as "peer blogging," where healthcare providers seek to reach out to their colleagues much as they do in offline channels such as medical journals or even professional conferences, discussing new treatments, drugs, or technologies.

The second is the "ranting" blog post, where physicians might vent about salaries, low health care reimbursement rates, long working hours, and other issues that frustrate them.[412] Such posts could generate unwelcome attention from peers, institutional providers, or medical boards. Suppose, for example, that a physician posted, "I had a case today dealing with a patient previously seen by Dr. Smith; I spent the best part of the day putting right what he did wrong!" Such a communication is likely to get the attention of the peer who could sue for defamation.[413] It might also attract scrutiny from professional organizations or

---

408. Tara Lagu et al., *Content of Weblogs Written by Health Professionals*, 23 J. GEN. INTERN. MED. 1642-46 (2008).

409. *Id.*

410. *Id.*

411. *See generally* Julia M. Johnson, *Web Risk: Blogging Can Be a Medically Useful Tool for Doctors; but Details Could Doom Your Career*, MO. MED. L. REP., June 2008 (interview with Nicolas Terry); Kennedy, *supra* note 400.

412. *See* Scott R. Grubman, Note, *Think Twice Before You Type: Blogging Your Way To Unemployment*, 42 GA. L. REV. 615 (2008); *see also* David Kravets, *AP Reporter Reprimanded For Facebook Post; Union Protests*, WIRED, June 9, 2009, *available at* http://wired.com/threatlevel/2009/06/facebooksword (discussing various adverse employment disciplinary actions brought by employers against Facebook-posting employees).

413.

> In a suit for defamation, a private plaintiff must allege (1) publication of false statements about the plaintiff that "expose [] [him] to distrust, hatred, contempt, ridicule or obloquy or which cause [him] to be avoided, or which [have] a tendency to injure [him] in his office, occupation, business or employment."

Saadi v. Maroun, No. 8:07-cv-1976-T-24-MAP, 2009 U.S. Dist. LEXIS 42574, *10 (M.D. Fla. May 20, 2009) (quoting Cooper v. Miami Herald, 31 So. 2d 382, 384 (Fla. 1947)). The plaintiff must also allege that the publication was "(2) done without reasonable care as to the truth or falsity of those statements; and (3) that result in damage to that person." *Id.* (citing Hay v. Indep. Newspapers, Inc., 450 So. 2d 293, 294-95 (Fla. Dist. Ct. App. 1984)). In *Saadi*, the court found that the defendant's allegations, published on a blog that the plaintiff was an unemployed lawyer and that his car was purchased with stolen money, to be triable whether they satisfy elements these three of a defamation suit. *Id.* at *11-12. The court further found that even though the blog was political in tone, there was a sufficient mix of fact and opinion as to be reasonably construed as

medical boards for unethical conduct,[414] and could violate the terms of a contract with an employing or credentialing healthcare institution.

The highest level of risk is associated with a blog posting that involves the risk of a patient being identified. Here, both the breach of confidence tort and HIPAA may be implicated. Physicians may use pseudo anonymous terms to describe the cases they reference in an attempt to reduce the possibility of positively identifying any patient in a blog discussion. Notwithstanding such efforts, re-identification may be possible from detailed demographics, location, as well as symptoms. Discussing general breaches of confidentiality, Brann and Mattson note, "[u]nintentional confidentiality breaches have been overheard in elevators, cafeterias, hallways, doctors' offices, and hospital rooms and at cocktail parties."[415] The authors' typology of breaches included disclosures by healthcare providers to their own family members[416] and to their friends.[417] As they describe in the latter context (which is analogous to social network posts),

> [i]n providing confidential information to friends, health care providers run an even greater risk of harming patients. This is because they may not be as aware of their friends' extended network of relationships as they are of their family's. Consequently, they may have even less control over who else might become privy to the confidential information.[418]

2. Twitter Feeds and Status Updates.—In February 2009, a surgeon at Henry Ford Hospital in Detroit provided a real-time Twitter feed during his performance of a robotic partial nephrectomy on a patient.[419] This was not a rogue surgeon indulging a personal interest. Dr. Craig Rogers is a well-known urologist and the feed, written by his chief resident, was publicized in advance

---

defamation. *Id.* at *14. In the example cited, the fact that the discussion would likely be predicated on an actual patient or health problem would make it easier for courts to find defamatory statements when mixed with opinion. Note also that First Amendment protection for derogatory blog posts is limited. *See, e.g.*, Richerson v. Beckon, 337 F. App'x 637 (9th Cir. 2009) (defense summary judgment upheld in § 1983 action by teacher against supervisor who was transferred after making comments on her personal blog), *amended by* 08-35310, 2009 U.S. App. LEXIS 19327 (Aug. 27, 2009).

414. *See, e.g.*, AMA CODE OF MEDICAL ETHICS § 9.031—Reporting Impaired, Incompetent, or Unethical Colleagues, http://www.ama-assn.org/ama/pub/physician-resources/medical-ethics/code-medical-ethics/opinion9031.shtml (specifying how such issues should be dealt with).

415. Maria Brann & Marifran Mattson, *Toward a Typology of Confidentiality Breaches in Health Care Communication: An Ethic of Care Analysis of Provider Practices and Patient Perceptions*, 16 HEALTH COMM. 231, 233 (2004) (citations omitted).

416. *Id.* at 244-45.

417. *Id.* at 245.

418. *Id.*

419. Elizabeth Cohen, *Surgeons send 'Tweets' from Operating Room*, CNN.COM, Feb. 17, 2009, http://www.cnn.com/2009/TECH/02/17/twitter.surgery/index.html.

by his hospital system.[420] The avowed purpose of the feed was "to get the word out" about less invasive surgical techniques.[421]

As previously noted, the AMA Code of Ethics mandates that either contemporaneous or recorded observations of physician-patient interactions must be preceded by explicit agreement and comprehensive informed consent. Separate consents are required both for the original recording and any subsequent broadcast. The consent must state that patient's decision will not affect the medical care he or she receives.[422]

These general rules are reinforced by various ethics opinions from specialty organizations.[423] For example, in answer to the question, "May I use a videotape segment of a therapy session at a work-shop for professionals?" the American Psychiatric Association listed the following preconditions:

1. The patient gives fully informed, uncoerced consent that is not obtained by an exploitation related to the treatment.
2. The proposed uses and potential audience are known to the patient.
3. No identifying information about the patient or others mentioned will be included.
4. The audience is advised of the editing that makes this less than a complete portrayal of the therapeutic encounter.[424]

The common law privacy rules are consistent. Recall *Vassiliades v. Garfinckel's, Brooks Brothers*, where a physician published before and after photographs of his patient via a television commercial.[425] The court found "[t]he nature of the publicity ensured that it would reach the public."[426] It seems reasonably clear that public Twitter feeds or unsecured Facebook pages will satisfy the courts' emerging approach to "public" disclosure as discussed in *Yath*.[427] As evidenced by the increased use of such feeds by public entities (such as police departments), this is a broadcast medium designed to reach the public.[428]

The specific difficulty faced by physicians using social network real-time broadcast technologies such as Twitter feeds or Facebook status updates is how

---

420. *Live Surgery on Twitter, Please Join Physicians from Henry Ford for Our Next Live Twitter Surgery Event on February 9th*, http://www.henryford.com/body.cfm?id=51168 (last visited Jan. 15, 2010).

421. Cohen, *supra* note 419.

422. *See supra* text accompanying note 230.

423. *See, e.g.*, AM. PSYCH. ASS'N, *supra* note 391, at 24.

424. *Id.*

425. *See supra* text accompanying note 179.

426. Vassiliades v. Garfinckel's, Brooks Bros., 492 A.2d 580, 588 (D.C. 1985).

427. *See supra* text accompanying note 325.

428. *See, e.g.*, Lisa Respers France, *Police Departments Keeping Public Informed on Twitter*, CNN.COM, Mar. 13, 2009. http://www.cnn.com/2009/TECH/03/13/police.social.networking/index.html; Jasmine Huda. *Law Enforcement Turns to Twitter*, KSDK.COM, June 19, 2009, http://www.ksdk.com/news/local/story.aspx?storyid=178164.

to satisfy the ethical and legal requirements of consent. Informed consent does not scale well and application of consent requirements analogous to filming or broadcasting patient treatments include quite specific (and close to impossible) requirements of the disclosure of the audience that will see the broadcast. Arguments that the patient was anonymous (or, in HIPAA terms, that the patient information was de-identified) may not be sustainable given the likelihood that some in a public audience would be able to deduce the identity of the patient.

One blogger has published "140 Health Care Uses for Twitter"[429] and, perhaps, physicians pushing status updates from an emergency room honestly believe that they are educating others about the practice of medicine. However, if either the tweeting or the blogging is about patients, the admonition from Nadelson and Notman requires reiteration; "what is best for the patient must be the physician's first priority."[430]

CONCLUSION

The issues examined in this article are about context. For many readers there may be no issue deserving of legal resolution—merely bemusement that anyone would act online in a manner analogous to wearing a t-shirt proclaiming "I Like Weed" or "If You Can Read This, I've Been Paroled" to a job interview. Similarly, it may be argued that the legal system should not rescue those with bad judgment or concern itself with risky behavior that is exposed to all by users who fail to make appropriate use of available privacy or security settings. As more people lose their jobs or their health insurance because of what they post online perhaps more users will employ these settings to disaggregate their "friends" or otherwise modulate their online behavior. Equally, healthcare institutions, teaching hospitals, and physician organizations are likely to make their views about the online behavior of their physicians far more pointed and embed them in normative form. From there such norms are likely to migrate to our legal and regulatory systems.

The soft (even soft law) answers to many of the issues discussed in this article are, first, to increasingly incorporate the issues raised into professional training and institutional risk management strategies. Second, observe as press and public opinion (combined with nudges from regulatory agencies such as the FTC) force social network sites to increase the number and transparency of protective online tools they make available to users. However, changes to their architectures, such that robust privacy and security settings become the default, challenge aspects of the services' business models and likely will not occur soon, or willingly. Third, whatever the EEOC ends up proposing with regard to social network data and GINA, we are likely to see legislatures or regulatory agencies fashion some bright lines as to when posted data can or cannot be used in some contexts or by some persons.

---

429. Phil Baumann, http://philbaumann.com/2009/01/16/140-health-care-uses-for-twitter/ (Jan. 16, 2009, 14:21).

430. *See supra* text accompanying note 391.

Beyond and, perhaps, before such amelioratory strategies, the common law of boundaries must step up and protect responsible users online. True to its context-based framework the law of boundaries should recognize private or secluded areas that have been established by users of social network sites.